Gesetz der Internetsicherheit und Industrie 4.0

BE SAFE ON THE INTERNET

Co-funded by the Erasmus+ Programme of the European Union

Inhaltsverzeichnis

Liste der Abkürzungen

APT: Advanced Persistent Threats (fortgeschrittene anhaltende Bedrohung)

CERT: Computer Emergency Response Team (Computersicherheits-Ereignis- und Reaktionsteam)

CNCS: Centro Nacional de Cibersegurança (Nationales Zentrum für Cybersicherheit in Portugal)

CSC: Cyber Security Center (Cybersicherheitszentrum)

CSIRT: Computer Security Incident Response Team (Reaktionsteam für Computersicherheitsverletzungen)

DDOS: Distributed Denial of Service (Verteilte Dienstblockade)

DSN: Digital Supply Network (Digitales Versorgungsnetz)

EU: European Union (Europäische Union)

GDPR: General Data Protection Regulation (Datenschutz- Grundverordnung – DSVO)

IKT: Kommunikations- und Informationstechnologie (Information and Communication Technology)

IDSA: Czech Institute of Informatics, Robotics and Cybernetics (Tschechisches Institut für Informatik, Robotik und Kybernetik)

IT: Information Technology (Informationstechnologie)

ÖSCS: Österreichische Strategie für Cybersicherheit

NCBI: NarodniCentrumBezpecnejsiholInternetu (Nationales Zentrum für das Internet PL)

SIC: Safer Internet Center

KMU: kleine und mittelständische Unternehmen (Small and Medium Enterprise SME)

Abbildungen

Schlüsseldefinitionen

Fortgeschrittenen anhaltende Bedrohungen: komplexe und gezielte Angriffe auf kritische IT-Infrastrukturen von Unternehmen und Behörden.

Botnetz: Sammlung Internet verbundener Geräten, zu denen Computer, Server, mobile Geräte und Internet-Geräte gehören können, die von einer gemeinsamen Art von Malware infiziert und kontrolliert werden.

Cybersicherheit: der Schutzes von Systemen, Netzwerken und Programmen vor digitalen Angriffen. Diese Cyberangriffe zielen in der Regel darauf ab, auf sensible Informationen zuzugreifen, sie zu verändern oder zu zerstören, Geld von Benutzern zu erpressen oder normale Geschäftsabläufe zu unterbrechen.

Datenverletzungen: eine absichtliche oder unabsichtliche Freigabe von sicheren oder privaten/vertraulichen Informationen an eine nicht vertrauenswürdige Umgebung. Datenverstöße können persönliche Gesundheitsinformationen, persönlich identifizierbare Informationen, Geschäftsgeheimnisse und/oder geistiges Eigentum betreffen.

Dienstverweigerungs- Angriff: ein Sicherheitsereignis, das eintritt, wenn ein Angreifer berechtigte Benutzer am Zugriff auf bestimmte Computersysteme, Geräte, Dienste oder andere IT-Ressourcen hindert.

Internetsicherheit: Wissen um die Maximierung der persönlichen Sicherheit und der Sicherheitsrisiken des Benutzers in Bezug auf private Informationen und Eigentum im Zusammenhang mit der Nutzung des Internets und den Selbstschutz vor Computerkriminalität im Allgemeinen.

Hoax/Kettenbrief: eine Falschmeldung, die über E-Mail, Instant Messenger, soziale

Netzwerke oder andere Mittel verbreitet wird. Böswillige Hoaxes sollen die Benutzer durch das Versenden zusätzlicher vielversprechender Links in Fallen locken, die jedoch nur Viren oder Malware verursachen oder zu betrügerischen Websites führen.

Malware (Schadsoftware): jedes Programm oder jede Datei, die für einen Computerbenutzer schädlich ist. Zu den Arten von Malware können Computerviren, Würmer, Trojaner und Spyware gehören. Diese bösartigen Programme können eine Vielzahl verschiedener Funktionen ausführen, wie z. B. das Stehlen, Verschlüsseln oder Löschen sensibler Daten, das Ändern oder Übernehmen von zentralen Computerfunktionen und das Überwachen der Computeraktivitäten der Benutzer ohne deren Zustimmung.

Phishing: Phishing ist eine Form des Betrugs, bei der sich ein Angreifer in einer E-Mail oder anderen Kommunikationskanälen als seriöse Einheit oder Person ausgibt. Der Angreifer verwendet Phishing-E-Mails, um böswillige Links oder Anhänge zu verbreiten, die eine Vielzahl von Funktionen erfüllen können, einschließlich der Extraktion von Anmeldeinformationen oder Kontoinformationen der Opfer.

Ransomware (Erpressungssoftware): bösartige Software, die darauf abzielt, den Zugang zu Archiven und Systemen zu blockieren, die für die Rückgabe des Zugriffs einen Wert verlangen.

Verleumdung (Slander): Falschaussage über jemanden, die ihren Ruf schädigt.

Spam: elektronische Nachrichtensysteme zum Versenden von unerwünschten Nachrichten in großen Mengen. Die häufigste Form von Spam ist E-Mail-Spam, aber der Begriff gilt auch für jede elektronisch versandte Nachricht, die unerwünscht und massenhaft ist.

Trojaner: Art von Malware, die oft als legitime Software getarnt ist. Trojaner können von Cyber-Dieben und Hackern eingesetzt werden, die versuchen, Zugang zu den Systemen der Benutzer zu erhalten.

Virus: ein Computervirus ist eine Art von bösartigem Code oder Programm, das geschrieben wurde, um die Funktionsweise eines Computers zu verändern, und das dazu bestimmt ist, sich von einem Computer auf einen anderen zu verbreiten.

Warez: Raubkopien von Software, wie z.B. illegal kopierte Software, oft nach Deaktivierung von Anti-Privatsphäre-Maßnahmen, die über das Internet verbreitet wird.

Wurm: Art von bösartigem Softwareprogramm, dessen Hauptfunktion darin besteht, andere Computer zu infizieren, während es auf infizierten Systemen aktiv bleibt.

1. Einführung

Industrie 4.0 wird zum einen verschiedene Veränderungen in Unternehmen fördern, weil es alle Ebenen der Produktions- und Lieferketten betrifft, einschließlich der Geschäfts- und Produktionsleiter, der Arbeitnehmer, der cyber-physischen Systeme, der Kunden, und zum anderen Bürger in ihrem Privatleben.

Die Vorteile, die sich aus der Industrie 4.0 ergeben, die Informationen und Vermögenswerte, die den Organisationen und Personen gehören oder von ihnen genutzt werden, werden immer wichtiger. Aus diesem Grund nimmt mit der neuen industriellen Revolution die Existenz von Angriffen exponentiell zu und bringt auch neue Risiken mit sich, die sowohl für die Organisationen als auch für die gesamte Gesellschaft berücksichtigt und thematisiert werden müssen. Deshalb sollte die Cybersicherheit zu einem integralen Bestandteil der Strategie, des Designs und des Betriebs werden, und die Umsetzung von Maßnahmen ist von nun an sehr wichtig. Es gibt eine Vielzahl von Maßnahmen/Praktiken, die in Unternehmen und im Privatleben der Bürger umgesetzt werden müssen, um die Sicherheit und den Schutz beim Sammeln, Schützen und Bereitstellen von Informationen zu verbessern. Darüber hinaus gibt es zwar einige Initiativen und Institutionen, die sich mit der Sicherheit im Internet befassen, aber es bleibt noch viel zu tun, vor allem weil die Welt heutzutage äußerst dynamisch ist und infolgedessen immer neue Bedrohungen entstehen, neue Schwachstellen entdeckt werden und die mangelnde Entwicklung/Schulung der Arbeitnehmer eine zentrale Herausforderung darstellt.

Die neue Ära der Digitalisierung bringt zunehmende Nutzung digitaler Technologien in noch mehr Bereichen von Wirtschaft und Gesellschaft und eine zunehmende Vernetzung von allem. Diese Situation ist auch verantwortlich für bedeutende soziokulturelle und wirtschaftliche, größere Herausforderungen und Bedrohungen auf Ebene der Sicherheit und einige politische Veränderungen im europäischen Gebiet. Daher ist es absolut notwendig, die Gesellschaft stärker für diese Realität zu sensibilisieren und besser auf sie vorzubereiten und einige Strategien auf nationaler Ebene einzubeziehen, die dazu beitragen sollen, eine sicherere Gemeinschaft im Alltag weltweit zu erreichen.

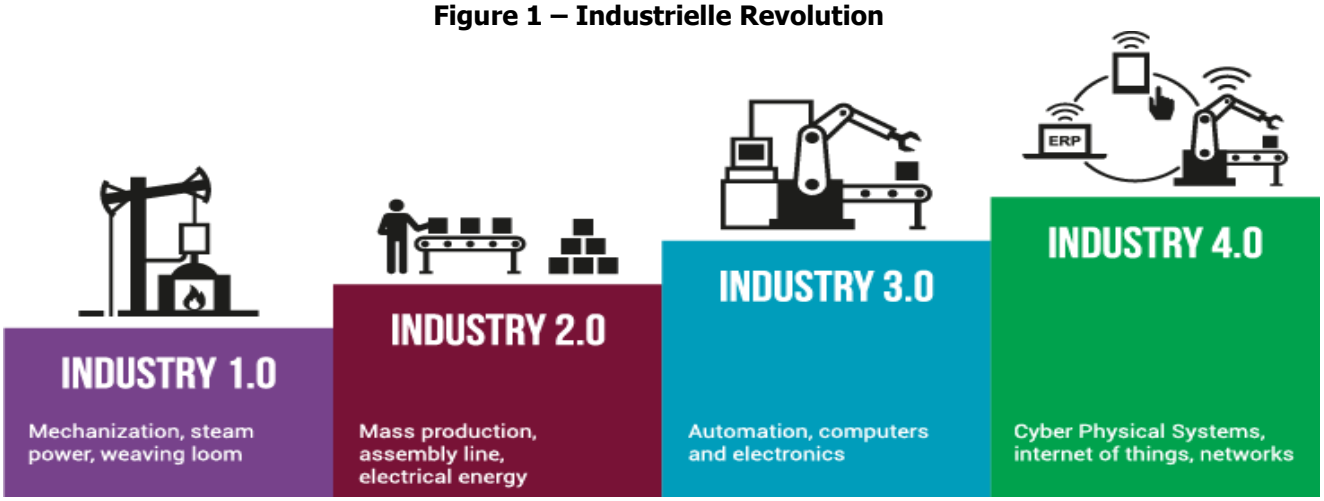
In diesem Bericht wird ein kurzer Überblick, über die wichtigsten Herausforderungen, denen

die Menschen in einigen europäischen Ländern tagtäglich gegenüberstehen, die Hauptrisiken/-schwierigkeiten, mit denen die Menschen täglich konfrontiert sind, die häufigsten Vorfälle in Bezug auf die Cybersicherheit und unsere Sicherheit, gegeben.

2. Industrie 4.0: eine kurze Übersicht

Die vierte industrielle Revolution, die gemeinhin als Industrie 4.0 bezeichnet wird, zeichnet sich durch dezentrale Intelligenz aus, die zu einer intelligenten Objektvernetzung und einem unabhängigen Prozessmanagement beiträgt, wobei die Interaktion der realen und virtuellen Welt einen entscheidenden neuen Aspekt der Fertigungs- und Produktionsprozesse darstellt.
In der Tat begann die Industrialisierung der Welt im späten 18. Jahrhundert mit der ersten industriellen Revolution und wurde durch die Einführung mechanischer Produktionsanlagen mit Hilfe von Wasser- und Dampfkraft definiert.
Die vierte industrielle Revolution ist gekennzeichnet durch die digitale Transformation mit der Entwicklung von cyber-physikalischen Technologien, die disruptive Veränderungen der Produktions- und Geschäftsmodelle ermöglichen.
Die Industrie 4.0 ist eine natürliche Folge der dritten industriellen Revolution, die die Natur des Handels in der zweiten Hälfte des 20. Jahrhunderts mit einer Reihe von Fortschritten in der Computerisierung und Informationstechnologie (IT) vollständig verändert hat. Es war eine Zeit großer Veränderungen für Einzelhandels- und Konsumgüterunternehmen, gekennzeichnet durch das Aufkommen von Kreditkarten, Back-Office- und Lagerautomatisierung, Just-in-Time-Lieferketten und die ersten Online-Geschäftsmodelle. Tatsächlich ist das Konzept von Industrie 4.0 relativ neu und hat in den letzten Jahren innerhalb der verschiedenen Unternehmen an Bedeutung gewonnen.

Figure 1 – Industrielle Revolution



Quelle: (Simio, n.d.)

Industrie 4.0 ist eine Kombination aus mehreren technologischen Fortschritten:

- **Informations- und Kommunikationstechnologie**: Die Digitalisierung und die weit verbreitete Anwendung der Informations- und Kommunikationstechnologie (IKT) ermöglichen die Integration aller Systeme über die gesamte Liefer- und Wertschöpfungskette hinweg und ermöglichen die Datenaggregation auf allen Ebenen. Informationen werden digitalisiert und die entsprechenden Systeme innerhalb und zwischen den Unternehmen in allen Phasen des Produktentstehungs- und Nutzungslebenszyklus integriert;

- **Cyber-physikalische Systeme:** Cyber-physikalische Systeme verbessern die Fähigkeit zur Steuerung und Überwachung physikalischer Prozesse mit Hilfe von Sensoren, intelligenten Robotern, Drohnen, 3D-Druckgeräten (einige davon werden in diesem Bericht ausführlicher behandelt). In cyber-physikalischen Systemen werden die physischen Komponenten zu einem Netzwerk von interagierenden Elementen zusammengefügt. Während die anfänglichen Eingänge und die endgültigen Ausgänge üblicherweise physisch sind, werden Informationen während des Herstellungsprozesses oft zwischen physischen und digitalen Zuständen ausgetauscht;

- **Netzwerk-Kommunikation**: All diese Geräte, sowohl innerhalb der Produktionsstätte als auch zwischen Lieferanten und Händlern, sind über verschiedene drahtlose und Internet-Technologien miteinander verbunden. Zuverlässige und qualitativ hochwertige Kommunikationsnetze sind eine entscheidende Voraussetzung für Industrie 4.0, und daher ist es wichtig, die Breitband-Internet-Infrastruktur dort zu erweitern, wo sie benötigt wird. Dieser hohe Vernetzungsgrad der miteinander verbundenen Komponenten ermöglicht einen dezentralen und selbstorganisierten Betrieb der cyber-physikalischen Systeme;

- **Big Data and cloud computing:** Durch den Einsatz von Big Data (Großdaten)und Cloud- Computing können die über diese Netze abgerufenen Informationen zur

Modellierung, Virtualisierung und Simulation von Produkten und Fertigungsprozessen genutzt werden;

- **Modellierung, Virtualisierung und Simulation:** Die Simulation ist eine Kernfunktionalität von Systemen durch nahtlose Unterstützung entlang des gesamten Lebenszyklus, z.B. durch Unterstützung von Betrieb und Service mit direkter Verknüpfung zu den Betriebsdaten;

- **Verbesserte Werkzeuge für die Mensch-Computer-Interaktion und Zusammenarbeit:** Um diese Prozesse zu steuern, werden den menschlichen Arbeitskräften modernste IKT-Werkzeuge zur Verfügung gestellt, die sich die Fortschritte der erweiterten Realität und der intelligenten Robotik zunutze machen. Die cyber-physikalischen Systeme von Industrie 4.0 haben das primäre Ziel, den Menschen bei seiner täglichen Arbeit zu unterstützen. Die Hauptmerkmale solcher Systeme sind Nicht-Aufdringlichkeit, Kontext-Anpassungsfähigkeit, Personalisierung, Ortsbezogenheit und Mobilität.

Darüber hinaus ist es wichtig, sich bewusst zu sein, dass es auch einige wichtige Herausforderungen im Zusammenhang mit Industrie 4.0 und Internetsicherheit gibt. Die beiden wichtigsten Herausforderungen sind:

- **Sicherheit:** Der vielleicht schwierigste Aspekt bei der Implementierung von Industrie 4.0-Techniken ist das IT-Sicherheitsrisiko. Diese Online-Integration bietet Raum für **Sicherheitsverletzungen**, **Datenlecks** und könnte sogar **Cyber-Diebstahl** beinhalten. Da die Daten in der gesamten Lieferkette gesammelt werden, werden sich Fragen des Eigentums ergeben, und es ist wichtig, dass Unternehmen sicherstellen, dass ihre Daten nicht in die Hände eines Konkurrenten gelangen. Andererseits muss sichergestellt werden, dass die Produktionsanlagen selbst keine Bedrohung für Mensch und Umwelt darstellen und dass die Mitarbeiter kontinuierlich Sicherheitsschulungen erhalten;

- **Privatsphäre:** Diese Frage betrifft nicht nur die Kunden, sondern auch die Hersteller. Einerseits muss der Kunde Daten sammeln und analysieren, die für die Entwicklung seines Unternehmens relevant sind. Andererseits könnte der Kunde das Gefühl haben, dass seine Privatsphäre bedroht wird. Auch kleine und große Unternehmen, die ihre Daten in der Vergangenheit nicht weitergegeben haben, müssen sich zu einer transparenteren Umgebung hinarbeiten. Die Überbrückung der Kluft zwischen dem Verbraucher und dem Produzenten wird für beide Seiten eine große Herausforderung sein.

2.1. Inwieweit wurde Industrie 4.0 an die Herausforderungen betreffend Internetsicherheit in Ihrem Land angepasst?

2.1.1. Österreich

Das Konzept von Industrie 4.0 treibt die Vernetzung von Maschinen über das Internet voran und öffnet so bisher geschlossene Systeme für neue Gefahren wie Cyber-Angriffe oder Malware. Der Schutz von IT-Systemen erfordert ein umfassendes Sicherheitskonzept und ein strategisches Informationssicherheitsmanagement.

Der Verband "Platform Industrie 4.0" ist sich der Bedeutung des Sicherheitsaspektes im Zusammenhang mit Industrie 4.0 bewusst und hat den Schwerpunkt "Security and Safety" ("Sicherheit und Gefahrenabwehr") im Strategiemeeting 2017 neu identifiziert.

Mit der Gründung der Expertengruppe "Security and Safety" will die Plattform Industrie 4.0 Österreich die Wahrnehmung der Bedeutung und des Stellenwerts des Themas Sicherheit für die Industrie 4.0 erhöhen, relevante Akteure in Österreich vernetzen und dazu beitragen, "Security & Safety" als einen österreichischen Wettbewerbsvorteil zu etablieren. Interessierten Mitgliedern und Experten aus Forschung und Industrie wird ein Forum für den Erfahrungsaustausch geboten und damit die Möglichkeit, ein gemeinsames Verständnis von Sicherheit in Bezug auf die Digitalisierung zu entwickeln. Als erstes gemeinsames Projekt ist die Erstellung eines österreichweiten Sicherheitskompetenzkataloges von Wissenschaft, privaten Forschungseinrichtungen und Unternehmen sowie eines Leitfadens "Industrielle Sicherheit" für Unternehmen geplant, mit dem Ziel, insbesondere kleine und mittlere

Unternehmen (KMU) für das Thema zu sensibilisieren, auf kritische Punkte im Bereich Sicherheit bei unternehmerischen Entscheidungen hinzuweisen und erste Hilfestellungen zu geben.

Die Implementierung von Industrie 4.0 ist ohne die Gewährleistung der Daten- und Softwaresicherheit nicht möglich. Daher ist es notwendig, neben der Weiterentwicklung der für Industrie 4.0 relevanten Sicherheitssysteme auch bestehende internationale Sicherheitsstandards zu nutzen, die ein professionelles Testen der eingesetzten Systeme und Software ermöglichen. IT-Sicherheit in der Industrie 4.0 erhält eine besondere Bedeutung durch die intensive Nutzung des Internets auch für Automatisierungssteuerungen, Virtualisierung und Cloud Computing, durch SelfX-Technologien (Selbstkonfiguration, Selbstheilung, Selbstoptimierung) und die agentenbasierte Vernetzung von intelligenten Funktionen untereinander.

Die Normenfamilie ISO/IEC 27000ff (entwickelt in ISO/IEC JTC 1/SC 27, IT-Sicherheitstechniken) bietet neben einem generischen Managementsystem für Informationssicherheit eine Vielzahl von allgemein akzeptierten und praxiserprobten Werkzeugen und themenspezifischen Lösungen wie ISO/IEC 27036-4 für die Sicherheit in Cloud-Diensten.

Die Norm IEC 62443 "Industrielle Kommunikationsnetze - Netzwerk- und Systemsicherheit", die im IEC /TC 65, Industrielle Prozessmesstechnik, Steuerung und Automatisierung, entwickelt wurde, basiert auf der Normenfamilie ISO/IEC 27000 (Verein Industrie 4.0 Österreich, 2016). Daher können wir bestätigen, dass es in Österreich zahlreiche Initiativen gibt, die darauf abzielen, die Herausforderungen der Industrie 4.0. und der Internetsicherheit zu verbessern.

2.1.2. Tschechien

Im Fall der Tschechischen Republik wird die Industrie 4.0 das Kerngeschäft der meisten Unternehmen in die digitale Welt verlagern. Die wichtigsten Herausforderungen für Unternehmen in der Tschechischen Republik sind Folgende:

- **IT-Sicherheit und Zuverlässigkeit von Schlüsselsystemen:** In einem Unternehmen, das von Maschinen verwaltet wird, wird es von entscheidender Bedeutung sein, dass die Daten der einzelnen Sensoren im Inneren der Maschinen

wirklich authentisch sind. Darüber hinaus ist es wichtig, dass die Einrichtung des Netzwerks nicht beeinträchtigt wird. Unternehmen werden von ihrer IKT-Infrastruktur abhängig;

- **Geschäftsprozessintegrität:** Der Druck auf den niedrigsten Preis und die kürzeste Zeit zur Umsetzung von Projektänderungen innerhalb von Industrie 4.0 kann sich negativ auswirken. Falsche Prozesseinstellungen können bei der Produktion und Lieferung von entscheidender Bedeutung sein. Diese Probleme können zu einem finanziellen Verlust oder sogar zu existenziellen Problemen des Unternehmens führen;
- **Empfindlichkeit gegenüber Softwarefehlern:** In vielen Unternehmen ist der Produktionsprozess weitgehend softwareabhängig, aber es gibt immer noch eine Beteiligung von Personen, die am Betrieb der Geräte beteiligt sind. Außerdem arbeiten Maschinen oder Anlagen in der Regel autonom (nicht an das globale System gebunden). In Zukunft werden die Maschinen durch eine zentrale Software verwaltet werden, die von der Funktion der Betriebssysteme, Firewalls, IDS / IPS-Schutz, Management-Tools usw. abhängt.

2.1.3. Portugal

In Portugal gab es in den letzten Jahren einige Initiativen zur Förderung der Branche 4.0 in Unternehmen. In diesem Zusammenhang hat die nationale Regierung in Portugal ein Programm namens "i4.0", das die nationale Reindustrialisierung fördern soll ins Leben gerufen. Diese Strategie umfasst mehr als 50 öffentliche und private Maßnahmen. Statistiken besagen, dass diese Maßnahmen in mehr als 50.000 Unternehmen, die in Portugal tätig sind, Auswirkungen haben werden und in einer ersten Phase die Requalifizierung und auch die Entwicklung digitaler Kompetenzen von mehr als 20.00 Arbeitnehmern ermöglichen werden.
Darüber hinaus sind die wichtigsten Herausforderungen der portugiesischen Unternehmen in Bezug auf die Anpassung an die Industrie 4.0 und die Internetsicherheit Folgende:

- **Der Mangel an digitalen Kompetenzen und die Neuqualifizierung des Personals -** diese Faktoren tragen zur Verzögerung der Entwicklung der digitalen Transformation und der Entwicklung der digitalen Reife bei und können einige Sicherheitsrisiken fördern;

- Der **Mangel an Personal, das in der Lage ist, die Implementierung und Wartung von Industrie 4.0-Lösungen zu planen, auszuführen und zu garantieren**. Um diese Situation zu lösen, können die Manager der Unternehmen Partnerschaften mit externen Organisationen, oder weiterführenden, technischen Schulen und Universitäten entwickeln;
- Der **Mangel an Fähigkeiten und Kompetenzen zur Erkennung von Sicherheitsmängeln** und deren Lösung. In Bezug auf dieses Thema erkennt die Mehrheit der Unternehmen, dass sie Sicherheitsmaßnahmen/Pläne umsetzen müssen, weil sie damit einen digitalen Transformationsprozess fördern;
- Die **Umstellung der alten Systeme auf die Technologien von Industrie 4.0 kann einige Sicherheitsrisiken mit sich bringen**, da die alten Systeme nicht für ein so hohes Maß an Konnektivität ausgelegt sind. Dies bedeutet, dass die Unternehmen zur Bewältigung der Sicherheitsrisiken den Schutz ihrer Systeme gewährleisten müssen. Sie müssen sich bewusst sein, dass sie neue Bedrohungen vermeiden und widerstandsfähig sein müssen, um Schäden zu begrenzen und ihren Betrieb wieder aufzunehmen. Wenn Unternehmen eine Strategie für Industrie 4.0 entwickeln, müssen daher alle Themen im Zusammenhang mit der Sicherheit ganz oben auf der Prioritätenliste stehen.

2.1.4. Spanien

Im Falle Spaniens ist die Schaffung einer Umgebung des digitalen Vertrauens, die eine Verstärkung des Schutzes der Institutionen ermöglicht und die Einbindung der Bürger in das digitale Umfeld fördert, für die Entwicklung einer vernetzten Gesellschaft von entscheidender Bedeutung. Um dies zu erreichen, muss die Cybersicherheitsindustrie als wichtigstes Element fungieren.

In diesem Zusammenhang prüft die spanische Agentur für Digitaltechnik, die sich auf das oben genannte Ziel konzentriert und insbesondere mit Hilfe des Digital Trust Plan, die Möglichkeit der Durchführung einer Machbarkeitsstudie in Zusammenarbeit mit den wichtigsten Referenzagenten und dem Nationalen Forum für Digitales Vertrauen mit dem Ziel, einen Integrationsvorschlag für die Gründung einer Cybersicherheitsindustrie zu entwickeln.

Nach der Umsetzung der DSGVO ist das Ziel nichts anderes als die Gewährleistung eines sichereren Umfelds für persönliche Daten und Informationen. Dieser Prozess stellt jedoch eine Herausforderung für die Unternehmen dar. Der neue Standard führt Instrumente ein, wie das Recht vergessen zu werden, die Verpflichtung in einer kurzen, verständlichen und einfachen Sprache zu informieren oder die Erleichterung der Übertragbarkeit der Daten auf ein anderes Unternehmen, das ohne Hindernisse beauftragt wurde. Vor allem ist die technologische Entwicklung mit einer stärkeren Exposition gegenüber neuen Bedrohungen verbunden, insbesondere solchen, die mit dem Cyberspace verbunden sind. Die Hyperkonnektivität der heutigen Welt verschärft einige Schwachstellen des Sicherheitssystems und erfordert einen größeren Schutz der Netzwerke und Systeme sowie der Privatsphäre und der digitalen Rechte der Öffentlichkeit. Spanien muss sich an diesen permanenten Wandel anpassen, indem es seine Anstrengungen zur Digitalisierung und Technisierung des Staates und der Gesellschaft auf der Grundlage eines an diese neue Realität angepassten Bildungs- und Ausbildungssystems verstärkt.

Um sich an den durch die neue europäische Datenschutzverordnung erforderlichen Wandel anzupassen, war es notwendig, einen Plan zu erstellen, der im Rahmen einer nationalen Strategie für die Cybersicherheit entwickelt wurde, die einen enormen Wandel in den Beziehungen zwischen Unternehmen, Bürgern und öffentlichen Einrichtungen mit sich brachte, um die Entwicklung der Gesellschaft zu fördern. Dies wurde ermöglicht durch:

- **Strategischer Plan für Cybersicherheit:** Das Hauptziel dieses strategischen Plans der spanischen Regierung konzentriert sich auf die Gewährleistung einer sicheren Nutzung von Informationssystemen und -netzen durch ein System zur Prävention, Analyse, Wiederherstellung und Aufdeckung von Cyberangriffen im Bereich der neuen Technologien. Auf diese Weise wird die nationale Gesetzgebung mit den im Rahmen des internationalen Rechts festgelegten Vorschriften in Übereinstimmung mit den von Spanien eingegangenen Verpflichtungen eingehalten. Andererseits konzentrieren sich die Herausforderungen einer globalen, vollständigen und flexiblen Reaktion auf die identifizierten Risiken und Bedrohungen.

- **Sicherheitsvorschriften und Normen:** Sicherheitsvorschriften und Normen: Wie von Europa definiert, wird der Datenschutz ab dem 25. Mai 2018 geregelt und verbindlich vorgeschrieben. Er legt die Umsetzung neuer Sicherheitsmaßnahmen für Freiberufler, Unternehmen und die öffentliche Verwaltung fest. Diese Maßnahmen umfassen die Einführung von Verschlüsselungs- und Zwei-Faktor-Basis-Authentifizierungssystemen, wenn das Risiko dies erfordert. In diesem Sinne ist es von entscheidender Bedeutung, sich an die LOPD anzupassen und den Inhalt von LSSICE zu kennen, sowie eine Datenschutzberatung zu unterstützen, um zu überprüfen, wie die Computersicherheitsmaßnahmen umgesetzt werden, und um zu wissen, welches Sicherheits- und Schutzniveau gegen jeden Angriff garantiert werden muss.

- **Allgemeine Datenschutzbestimmungen:** Das Recht der neuen Technologien stellt einen großen Fortschritt in Bezug auf die Dokumentation dar, doch wir sollten verstehen, dass wir eine neue konzeptuelle und rechtliche Realität leben. Andererseits muss man bedenken, dass durch Computerangriffe täglich eine große Menge vertraulicher Informationen gestohlen werden kann. Die Unternehmen haben präventive und schützende Instrumente eingeführt, um jeden Eindringling vom Zugang zu ihren Informationen fernzuhalten. Zusammengefasst besagen die Allgemeinen Datenschutzbestimmungen, dass Unternehmen versuchte Einbrüche und erfolgreiche unbefugte Zugriffe sowie betroffene Daten melden müssen. Diese Cybersicherheitsmaßnahmen garantieren eine größere Kontrolle und einen besseren Schutz der privaten Informationen.
    - Einige technologische/systemische/organisatorische Herausforderungen sind:
        - **Verbesserung der Cybersicherheits-Fähigkeiten** von Regierungen, Behörden, Organisationen, Universitäten usw., um den Stand der Technik im Bereich der industriellen Cybersicherheit zu erreichen;
        - **Das allgemeine Bewusstsein schärfen und spezielle Schulungen anzubieten,** die für jede Art von Benutzer geeignet sind;
        - **Entwicklung von Instrumenten zur Erleichterung öffentlich-privater Partnerschaften** auf allen Ebenen;

- Verstärkte Forschung zur industriellen Cybersicherheit;
- **Entwicklung von Cybersicherheitsstrategien** für die Industrie;
- **Entwicklung von Best-Practice-Richtlinien** und Referenzstandards;
- **Gründung von Testlabors**;
- **Entwicklung von Bewertungsschemata**;
- **Entwicklung von ICS-ZERTIFIKATIONEN (ICS-CERTs)**;
- **Unterstützung bei der Entwicklung von Regulierungsrahmen**;
- **Entwicklung von Systemen, die Cybersicherheit** vom Entwurf an **beinhalten**;
- **Entwicklung einer Cybersicherheitskultur** innerhalb der Säulen des traditionellen Arbeitsschutzes;
- **Herangehensweise und Ausbildung** der Personen, die für Kontrollsysteme in IKT-Sicherheitssystemen verantwortlich sind und umgekehrt;
- **Verbesserung der Einhaltung von Rechtsvorschriften**;
- **Verbreitung von Produkten und Lösungen** im Bereich der industriellen Cybersicherheit unter allen Beteiligten.

2.2. Wie war die Anpassung der Unternehmen und der gesamten Gesellschaft in Bezug auf die Cybersicherheit?

2.2.1. Österreich

Im zweiten Quartal 2015 veröffentlichten PwC und Strategy& gemeinsam die Studie "Industrie 4.0 - Österreichs Industrie im Wandel". In dieser Studie wurden österreichweit 100 Unternehmen aus fünf Branchen (Automobilzulieferer, Elektrotechnik und Elektronik, Maschinen- und Anlagenbau sowie der Prozessindustrie) befragt. Für eine erfolgreiche, zeitnahe Umsetzung der Konzepte der Industrie 4.0 müssen die Unternehmen noch zahlreiche Herausforderungen meistern. Für ein Drittel der Befragten stehen hohe Investitionen und eine oft unklare Wirtschaftlichkeitsberechnung sowie fehlende Standards und Normen für neue Industrie 4.0-Anwendungen im Vordergrund. Viele Unternehmen haben noch keine konkreten

Umsetzungspläne für Industrie 4.0-Lösungen erstellt oder Investitionen genehmigt, nachdem die Lösungen für viele Unternehmen neu sind, erhebliche Änderungen erfordern und das Potenzial schwer zu quantifizieren ist. Es besteht ein akuter Bedarf an mehr Transparenz und einem branchenübergreifenden Erfahrungsaustausch. Auch die internationale Standardisierung im Bereich der Industrie 4.0-Anwendungen muss gefördert werden, denn nur so kann die Zusammenarbeit zwischen den Unternehmen intensiviert und die Effizienz in Zukunft gesteigert werden. Die wichtigsten Herausforderungen sind:

- **Unzureichende Qualifikation der Mitarbeiter;**
- **Datenschutz;**
- **Datensicherheit.**

Der digitale Wandel wird die Anforderungen an die Mitarbeiter auf allen Stufen der Wertschöpfungskette von der Entwicklung über die Produktion bis zum Vertrieb verändern, und die zunehmende Digitalisierung wird Prozesse und Geschäftsmodelle agiler und datengetriebener machen. Dies erfordert von den Mitarbeitern völlig neue Fähigkeiten und Qualifikationen. Auch der Bedarf an Software-Entwicklern und Datenanalysten in der Industrie wird in den nächsten fünf bis zehn Jahren deutlich steigen (Busch et al., 2015).
Die Anpassung der Unternehmen und der gesamten Gesellschaft in Bezug auf Cybersicherheit ist bereits im Gange, aber weitere Anpassungen und das Engagement nicht nur der Behörden, sondern auch der einzelnen Unternehmen und jedes Einzelnen, der in dieser Gesellschaft lebt, sind erforderlich. Verschiedene Initiativen, wie der Verband Plattform Industrie 4.0 und die Kommission für Informationssicherheit, helfen in dieser Hinsicht durch Beratung. Da sich die digitalen Möglichkeiten ständig weiterentwickeln und verändern, besteht auch in Bezug auf Sicherheit ein Bedarf an kontinuierlicher Entwicklung.

2.2.2. Tschechien

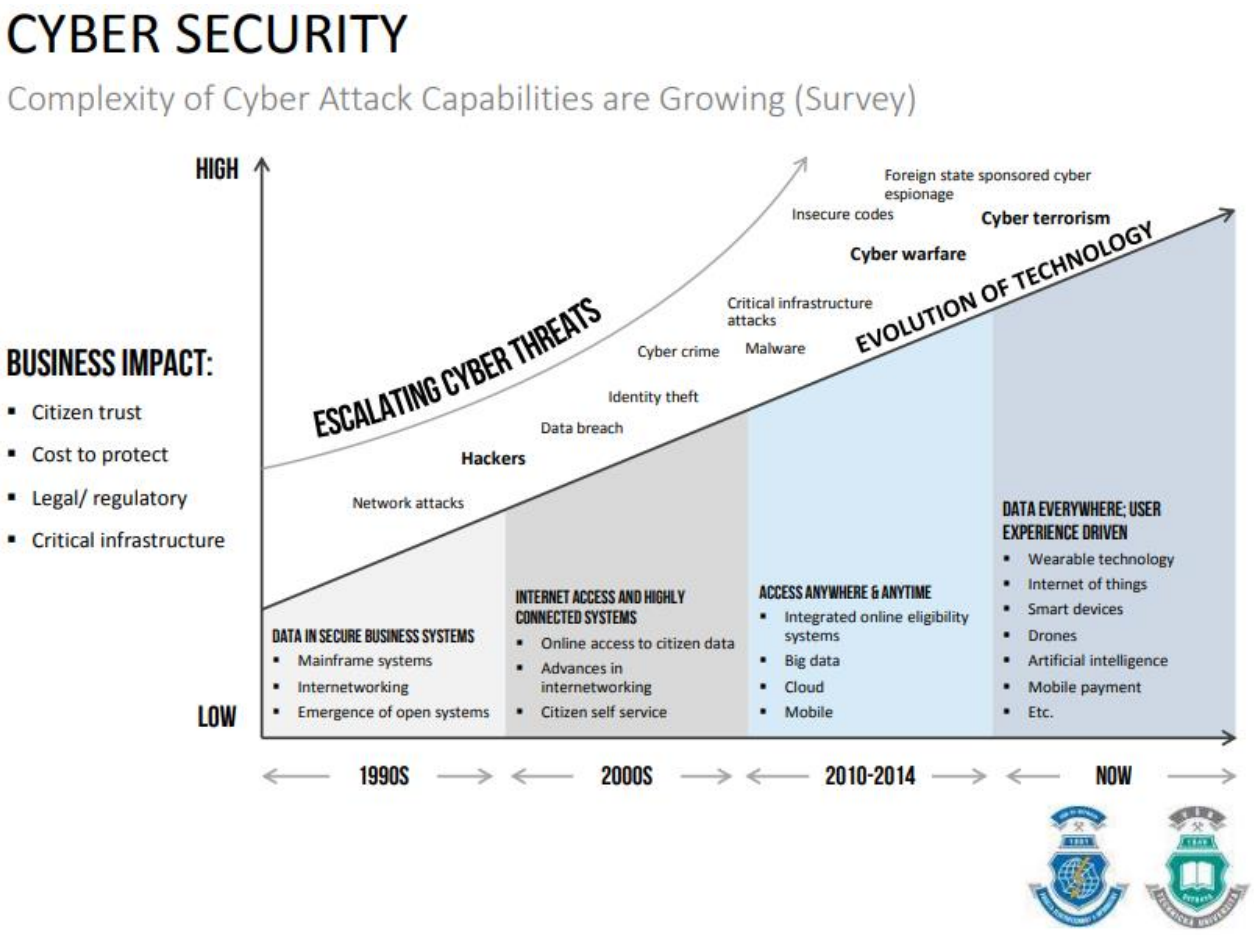
In Bezug auf die Anpassung der Unternehmen und der gesamten Gesellschaft in Bezug auf die Cybersicherheit gibt es einige geschäftliche Auswirkungen, die zum Beispiel die Unternehmen betreffen:

- **Vertrauen der Bürger;**

- **Zu schützende Kosten;**
- **Rechtliche/regulatorische Auswirkungen;**
- **Kritische Infrastruktur.**

Die Fakultät für Elektrotechnik und Informatik der VŠB-TUO in der Tschechien analysierte die eskalierenden Cyber-Bedrohungen im Laufe der technologischen Entwicklung von 1990 bis 2018, es wurde festgestellt, dass die Komplexität der Cyber-Angriffsmöglichkeiten wächst. In der nächsten Abbildung sehen wir die Ergebnisse dieser Bedrohungen.

Abbildung 2 - Bedrohungen im Cyberspace



Quelle: (VŠB-TUO, n.d.)

Wie wir in der obigen Abbildung sehen können, nimmt die Zahl der Cybersicherheitsprobleme seit 1990 zu. Mit der Entwicklung der Technologie eskalieren die Cyber-Bedrohungen und nach 2010-2014 sind die wichtigsten kritischen Cyber-Bedrohungen:

- **Malware;**
- **Angriffe auf die kritische Infrastruktur;**
- **Cyber-Kriegsführung;**
- **Unsichere Codes**;
- **Cyber-Terrorismus;**
- **Cyber-Spionage, die von ausländischen Staaten gefördert wird**.

2.2.3. Portugal

Der schnelle digitale Wandel bringt ein neues Problem im Zusammenhang mit der Cybersicherheit mit sich.

Das Centro Nacional de Cibersegurança (CNCS) hat sich zum Ziel gesetzt, einen sicheren nationalen Cyberspace zu gewährleisten und arbeitet in verschiedenen Phasen, insbesondere in der Reaktionsphase, d.h., wenn etwas schief geht. Es ist die formale Instanz, die für die nationale Cybersicherheit verantwortlich ist. Darüber hinaus wird der CNCS ein Instrument namens **"Modelos de Maturidade para a Cibersegurança"** schaffen, das eine Reihe von Maßnahmen und Kontrollen zur Anwendung bringen und einige Prioritäten definieren wird, um die Cybersicherheit weiter zu verbessern. Dieses Instrument wird in vier Dokumente unterteilt sein: 1) Wie man auf Vorfälle reagiert; 2) Wie man Vorfälle verhindert; 3) Wie man Vorfälle entdeckt; und 4) Management von Sicherheitsinformationen. Dieses Instrument wird 2019 zur Verfügung stehen und auch einige gute Praktiken enthalten, die sicherlich sehr hilfreich sein werden.

Der CNCS spielt auch bei diesem Thema eine sehr aktive Rolle und hat im Februar 2019 einen kostenlosen Online-Kurs ins Leben gerufen, der darauf abzielt, das Wissen und die Kompetenz im Bereich der Sicherheit zu erhöhen, wobei Themen wie Software-Update, Verwendung von Pen-Drives und Passwörtern, Verwendung im persönlichen und beruflichen Kontext behandelt werden.

Außerdem arbeitet der CNCS mit **nationalen und internationalen Kooperationsprogrammen**. Tatsächlich verfügt Portugal in diesem Bereich über eines der größten Kooperationsnetzwerke, um auf Cybersicherheitsvorfälle in Europa zu reagieren. Dieses Zentrum wurde erst 2014 gegründet.

Die Mehrheit der Cybersicherheitsereignisse kommt von dort:

- **Interne Zwischenfälle, da Beschäftigte manchmal ohne böse Absicht ein Verhalten oder eine Grundhaltung haben, die zu einigen Zwischenfällen führen können.** Aus diesem Grund ist die Bereitstellung von Schulungsaktivitäten für alle Beschäftigten von entscheidender Bedeutung, um einige der Zwischenfälle zu vermeiden, die passieren können. Obwohl die Investitionen in Schulungen von grundlegender Bedeutung sind, dürfen die digitalen Infrastrukturen, wie Software und Hardware, nicht vergessen werden, da sie zu mehr Sicherheit der Informatiksysteme führen;
- **Phishing- Angriff.** die Portugiesen investieren wenig in die Cybersicherheit und sind daher anfälliger für Angriffe. Dies geschieht, weil die Mehrheit der Unternehmen es immer noch vorzieht, die Dinge intern zu regeln, weil sie der Ansicht sind, dass dieser Bereich noch keine Priorität hat. Dies lässt sich durch die Tatsache erklären, dass die Mehrheit der portugiesischen Unternehmen KMUs sind;
- **Veraltete Technologie und Cybersicherheit** sind zwei Aspekte, die nach Ansicht jedes Managers den Fortschritt ihrer Unternehmen blockieren. Darüber hinaus bestätigen portugiesische Organisationen, dass die Cybersicherheit als Produktivitätsbremse wirkt, wobei fast die Hälfte der Technologie- und Unternehmerführer der Ansicht sind, dass die Cybersicherheit einen schlechten Einfluss hat;
- **Authentisierungs-Sicherheitsverfahren sind komplex oder verbrauchen mehr Zeit** wenn sie eine dringende Aufgabe erfüllen müssen oder wenn sie sich bei besonders knappen Fristen ermutigt fühlen, nicht konforme Wege zu gehen und "Abkürzungen" zu wählen;
- **Der Mangel an digitalen Kompetenzen und Fähigkeiten** ist immer noch ein großes Problem, obwohl es mehr Informationen und Initiativen online und offline gibt, die von öffentlichen und privaten Institutionen durchgeführt werden und darauf abzielen, ein sichereres Verhalten und eine sicherere Einstellung zu fördern. Dennoch fühlt sich vor allem die jüngere Generation immer wohler und verfügt über mehr Wissen, um mit Problemen der Cybersicherheit umzugehen.

Aus diesem Grund **sollten Unternehmen einige klare Sicherheitsstrategien verfolgen, die den Kunden Sicherheit geben**, und sie sollten einige Lösungspläne parat haben, wenn es zu einer Cybersicherheitskrise kommt.

Abschließend können wir sagen, dass Portugal in den letzten Jahren einige Initiativen im Zusammenhang mit der Cybersicherheit durchgeführt hat, und es gibt auch einige Initiativen, die darauf abzielen, ein viel sichereres Verhalten und eine sicherere Haltung der gesamten Gesellschaft zu fördern. Es gibt jedoch noch viel zu tun, um ein sichereres Umfeld sowohl in den Unternehmen als auch im Privatleben der Bürger zu schaffen.

2.2.4. Spanien

Cybersicherheitsprojekte in Spanien zielen darauf ab, die Sicherheit aktueller Anwendungen, Dienste und Infrastrukturen zu erhöhen und die Schaffung führender Märkte in Europa zu unterstützen, immer mit einem Endbenutzer-Ansatz und unter Einbeziehung aller für die Einhaltung der Vorschriften zuständigen Stellen, wie der Betreiber kritischer Infrastrukturen, der Anbieter von IKT-Diensten, der IKT-Händler, der Marktteilnehmer und der Bürger. All dies erfordert eine Stärkung der Kapazitäten zur Bewältigung von Bedrohungen aus dem Cyberspace. Daher sollte es zweckmäßig sein für:

- **Stärkung der Kapazitäten zur Ermittlung und Verfolgung von Cyberkriminalität,** zur Gewährleistung der Sicherheit der Bürger und des Schutzes der Rechte und Freiheiten im Cyberspace;
- **Förderung der Cybersicherheit von Bürgern und Unternehmen**;
- **Förderung der spanischen Cybersicherheitsindustrie,** um die Generierung und den Erhalt persönlicher Talente zu gewährleisten und so die digitale Autonomie zu stärken;
- **Beitrag und Förderung eines offenen, pluralistischen, sicheren und zuverlässigen Cyberspace,** der die nationalen Interessen unterstützt;
- **Entwicklung einer Cybersicherheitskultur**.

3. Internetsicherheit und Industrie 4.0: in Unternehmen

Es wird erwartet, dass die Technologien von Industrie 4.0 eine weitere Entwicklung der traditionellen linearen Lieferkettenstruktur durch die Einführung intelligenter, miteinander verbundener Plattformen und Geräte im gesamten Ökosystem anstoßen werden, was zu einem digitalen Liefernetzwerk (DSN) über die gesamte Wertschöpfungskette hinweg führen wird, über das sich die Unternehmen gegenseitig informieren können. Das Ergebnis könnte eine bessere Verwaltung und ein besserer Fluss von Materialien und Gütern, eine effizientere Nutzung von Ressourcen und Lieferungen sein, die den Kundenbedürfnissen besser gerecht werden. Neben all den damit verbundenen Vorteilen bringt die zunehmende Vernetzung des DSN auch Cyber-Schwächen mit sich, die in jeder Phase - vom Design bis zum Betrieb - richtig geplant und berücksichtigt werden sollten, um erhebliche Risiken zu vermeiden.

Aber ein reaktionsfähiges, agiles Netzwerk dieser Art wird nur durch den offenen Datenaustausch aller Teilnehmer des Versorgungsnetzes ermöglicht, was erhebliche Probleme schafft und zu einigen Schwierigkeiten zwischen der Transparenz einiger Daten und der Pflege der Informationen führen kann.

Aus diesem Grund sollten Organisationen Möglichkeiten zur **Sicherung dieser Informationen in Betracht ziehen, um zu verhindern, dass unberechtigte Benutzer** über das Netzwerk auf diese zugreifen, insbesondere wenn es um die Unterstützung von Prozessen wie die gemeinsame Nutzung von Informationen und den Systemzugang geht.

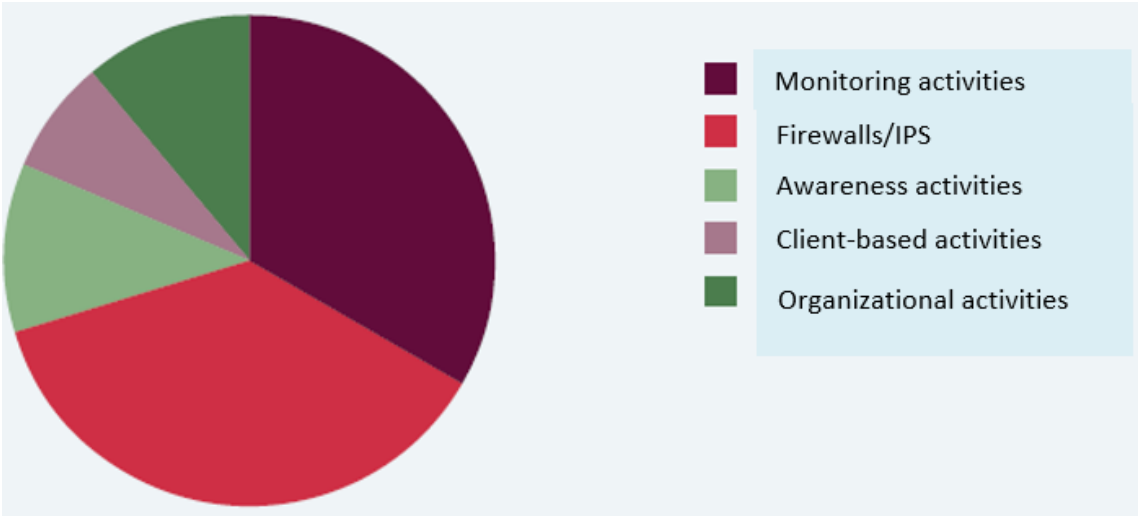
Der wichtigste Faktor, den es zu beachten gilt, ist Vertrauen. Organisationen müssen möglicherweise ihr **Risikomanagement ständig weiterentwickeln, um die Integrität zu wahren** und bei der Transaktion von Informationen oder Gütern sicher zu bleiben, sowie ihre Überwachungskapazitäten und Cybersicherheitsoperationen verstärken, um wachsam zu bleiben und nicht validierbare Prozesse zu schützen.

3.1. Welche Fälle im Zusammenhang mit der Internetsicherheit wurden in Ihrem Land in den letzten Jahren in Unternehmen gelöst?

3.1.1. Österreich

In Österreich gibt es einige Beispiele für Pannen im Zusammenhang mit der Internetsicherheit, wie z.B. Advanced Persistent Threats (APT). Im Oktober 2018 wurde Österreich Opfer eines solchen Angriffs mit dem Ziel, die Sicherheit der IT-Systeme von Behörden und Institutionen zu gefährden und Daten in großem Umfang zu stehlen. Die Angreifer nutzten verschiedene Kanäle, um die Opfer mit Malware zu infizieren, um Benutzerdaten zu manipulieren, mit dem letztendlichen Ziel, in Computernetzwerke einzudringen und vertrauliche Daten zu stehlen.
Die Vorkehrungen der angegriffenen Institutionen und die gute Zusammenarbeit zwischen GovCERT und Cyber Security Center (CSC) ermöglichte es, die Angriffe aller Betroffenen abzuwehren und den Datenabfluss zu verhindern. Die Tatsache, dass die Auswirkungen trotz der Anstrengungen der Angreifer minimal geblieben sind, ist ein weiteres Zeichen für die Wirksamkeit und Bedeutung einer kontinuierlichen Zusammenarbeit zwischen allen relevanten Stellen auf nationaler Ebene (Cyber Sicherheit Steuerungsgruppe, 2019).
In der nächsten Abbildung gibt es einen Überblick über die eingeführten Sicherheitsmaßnahmen.

Abbildung 3 – getroffene Maßnahmen (2018)

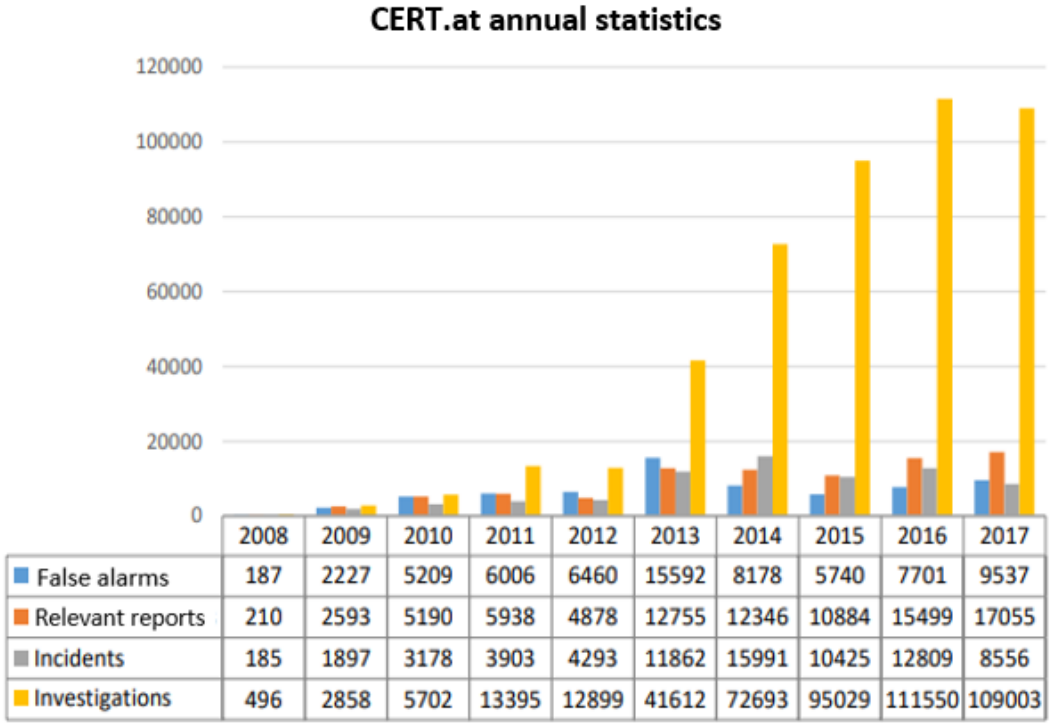


Quelle: (Cyber Sicherheit Steuerungsgruppe, 2019)

Während der technische Fortschritt in den Bereichen Firewalls/IPS und Endpoint-Schutz zweifellos zu einer Aufwertung der Abwehrmaßnahmen geführt hat, setzt sich auch hier der Trend des letzten Jahres fort: Statt auf reine Isolation zu setzen, tendieren immer mehr

Organisationen dazu, **Maßnahmen zur Erkennung von Angreifern in den eigenen Netzwerken zu überwachen**. Dazu gehört auch die **aktive Suche nach aktuellen Bedrohungen für die jeweilige Organisation** und in einem zweiten Schritt die gezielte Überprüfung der Systeme auf Infektionen. Darüber hinaus wurden vielerorts vorbereitende Maßnahmen getroffen, um Sicherheitsvorfälle mit forensischen Methoden analysieren zu können (Cyber Sicherheit Steuerungsgruppe, 2019).

Abbildung 4 - Jahresstatistik mit Überblick über Berichte, Vorfälle und Untersuchungen im Zeitablauf



	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
False alarms	187	2227	5209	6006	6460	15592	8178	5740	7701	9537
Relevant reports	210	2593	5190	5938	4878	12755	12346	10884	15499	17055
Incidents	185	1897	3178	3903	4293	11862	15991	10425	12809	8556
Investigations	496	2858	5702	13395	12899	41612	72693	95029	111550	109003

Quelle: (Nic.at GmbH, 2018)

Seit 2008 leitet das Computer Emergency Response Team (CERT).at Team die jährliche Gesamtstatistik. Diese umfasst die Anzahl der relevanten Berichte, Vorfälle und Untersuchungen sowie Fehlalarme. Von 2008 bis 2017 arbeitete CERT.at an der kontinuierlichen Verbesserung der Cybersicherheit in Österreich. In Abbildung 4 kann man die Anzahl der Berichte, Vorfälle und Untersuchungen im Laufe der Zeit sehen und es kann bestätigt werden, dass die Anzahl der relevanten Berichte deutlich größer ist als die der übrigen Kategorien. Die Erklärung für jede der folgenden Kategorien wird weiter unten

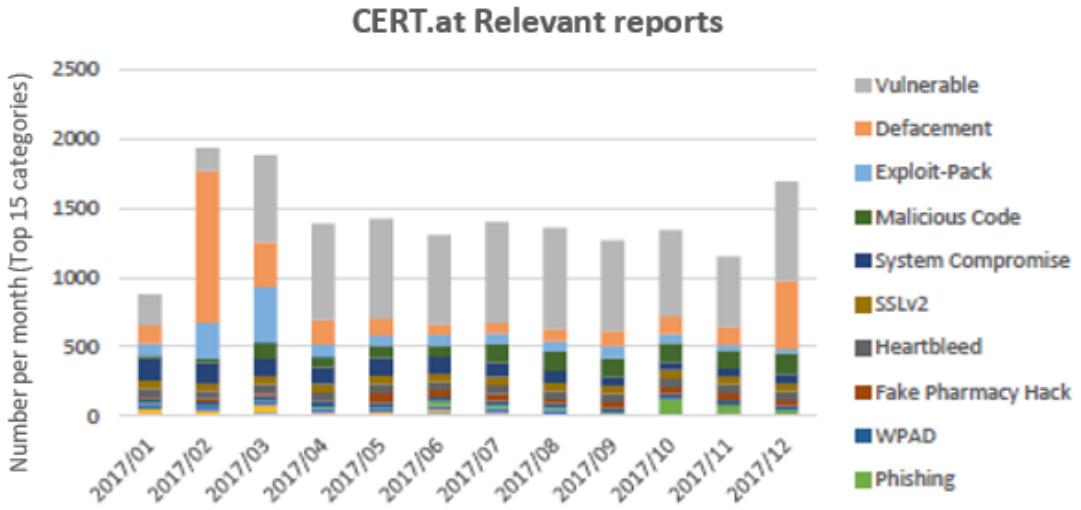
dargelegt.

"Relevant Report" ("relevante Meldungen") beziehen sich auf eingehende Meldungen an CERT.at, nicht alle beschreiben eine Situation, die CERT.at als relevantes Ereignis klassifiziert und aktiv behandelt werden muss.

"Incidents" ("Vorfälle") sind jene Fälle, die tatsächlich ein Sicherheitsrisiko darstellen. In diesen Fällen wird CERT.at aktiv und informiert betroffene Unternehmen, Organisationen oder Privatanwender z.B. über IT-Sicherheitsbedrohungen und unterstützt sie in besonderen Fällen bei der Problemlösung.

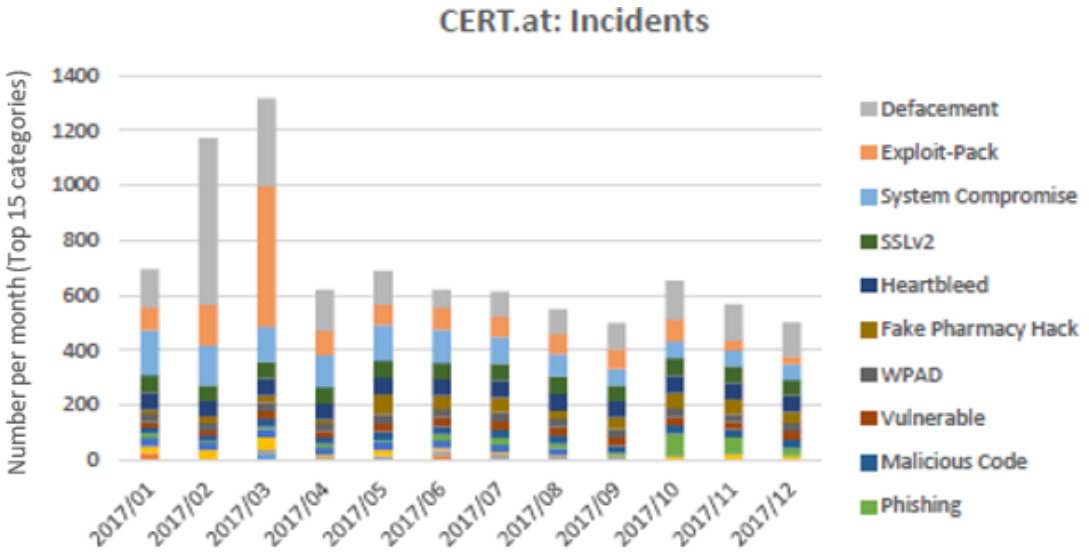
Im CERT.at Ticketsystem wird die Kontaktaufnahme mit den betroffenen Unternehmen, Organisationen oder privaten Nutzern als "Investigation" ("Untersuchung") bezeichnet. Eine Untersuchung ist in der Regel eine E-Mail an den Netzbetreiber, Webhoster oder Domaininhaber. In den Abbildungen 5, 6 und 7 gibt es einen Überblick über die häufigsten Vorfälle, die sich im Jahr 2017 ereignet haben, nach Kategorien.

Abbildung 5 - Klassifikation relevanter Berichte nach Bedrohungsart im Zeitablauf (2017)



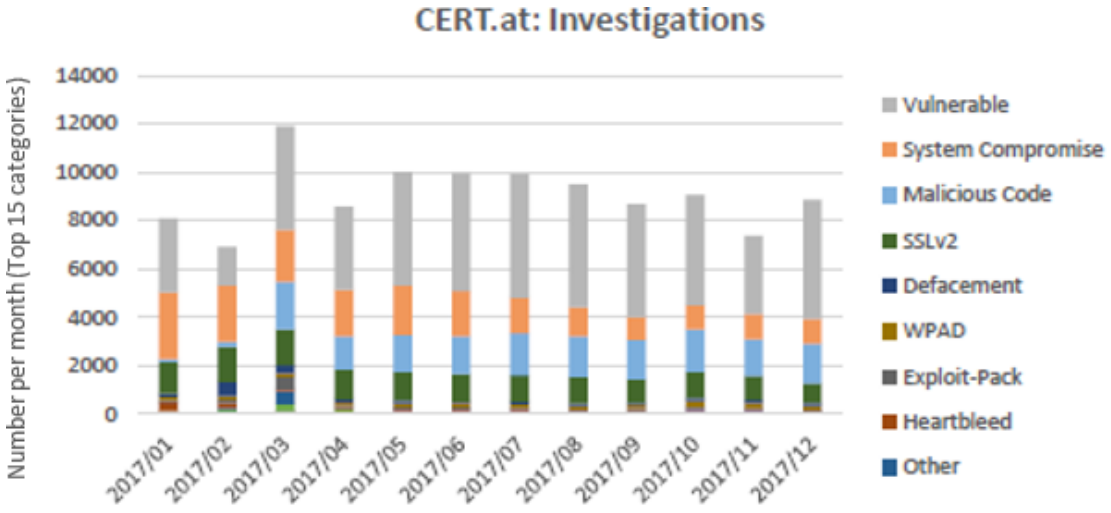
Quelle: (Nic.at GmbH, 2018)

Abbildung 6 - Klassifikation von Vorfällen nach Bedrohungsarten im Zeitablauf (2017)



Quelle: (Nic.at GmbH, 2018)

Abbildung 7 - Klassifikation der von CERT.at durchgeführten Untersuchungen nach Bedrohungsformen im Zeitablauf (2017)



Quelle: (Nic.at GmbH, 2018)

3.1.2. Tschechien

Eine nationale Analyse der Fälle von Internet-Kriminalität in der Tschechischen Republik ergab, dass Folgende zu den bedeutendsten Manifestationen von Cyberkriminalität gehören:

- **Betrug und Veruntreuung;**

- **Fälschung;**
- **Verleumdung;**
- **Elektronische Rache;**
- **Hoaxes;**
- **Warez;**
- **Systemdurchbrüche;**
- **Computer-Banküberfall (Phishing, Pharming, IP-Spoofing)**

Die Cyberkriminellen haben sich wieder verlagert und ihre Methoden sind ausgefeilter als früher, und viele Unternehmen und Institutionen sind auf die aktuellen modernen elektronischen Angriffe nicht vorbereitet. Die Polizei der Tschechischen Republik beobachtet seit 2011 die Entwicklung der im Cyberspace (vor allem im Internet) begangenen Straftaten. Die Fälle von Cyberkriminalität nehmen seitdem stetig zu (von etwa 1500 Verbrechen im Jahr 2011 auf mehr als 5.650 Verbrechen im Jahr 2017), das Wachstum hat sich in den letzten Jahren verlangsamt. Die CRIS.CZ-Vorfälle im Jahr 2017 zeigen, dass dadurch die größten Bedrohungen bestehen:

- **Phishing;**
- **Malware;**
- **Spam;**
- **Trojaner.**

Der häufigste Angriff ist Phishing durch die Beschaffung sensibler Informationen wie Kreditkartennummern oder Passwörter von Konten. Aber auch gefälschte E-Mails von Firmenchefs sind häufig mit dem Befehl, einen bestimmten Geldbetrag auf ein bestimmtes Konto zu überweisen.

3.1.3. Portugal

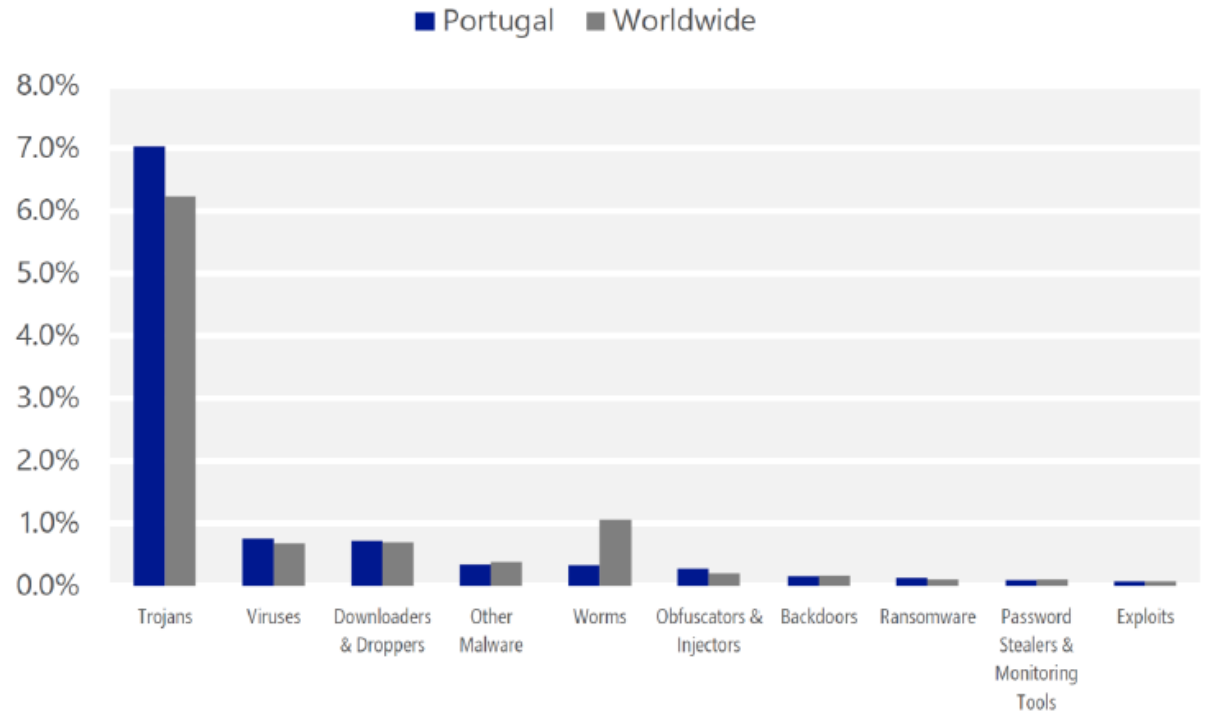
In Portugal sind die häufigsten Angriffe:

- **Phishing-Angriffe,** die im Allgemeinen von SPAM-Nachrichten gefolgt werden, die an mehrere Benutzer gesendet werden. Es mag zwar Phishing-Arten geben, bei denen

die Daten direkt als Antwort auf die E-Mail angefordert werden, aber am häufigsten werden sie mit einer Website artikuliert, auf der Sie Ihre Daten eingeben. Laut der Studie "Spam and Phishing in 2018", die von Kaspersky Lab über die Online-Sicherheit durchgeführt wurde, war Portugal das Land den zweithäufigsten Phishing-Angriffen;

- **Cyber- Sicherheitsverletzungen (gestohlene Daten);**
- **Die "Ransomware"-Angriffe** gingen 2018 in Portugal zurück, und Phishing bleibt die bevorzugte Angriffsmethode. Auch bei der Aufdeckung von Cybersicherheitsverletzungen liegt Portugal immer noch etwas unter dem internationalen Durchschnitt, mit Ausnahme der Identifizierung von Krypto-Münznzerei-Episoden.;
- **Malware and Trojaner.** Laut einem Bericht von Gabinete de Estratégia e Estudos ist Portugal eines der Länder mit einer der höchsten Malware-Vorfallsraten, und dies ist die in Portugal neben Trojanern am häufigsten vorkommende Schadsoftware (siehe Abbildung 8).

Abbildung 8 - Vorfallsrate bösartiger Software (März 2017)



Quelle: Microsoft (2018)

- **Cloud- Bedrohungsinformation ("cloud" Bedrohung)** ist derzeit eine der jüngsten

Bedrohungen für die Informationssicherheit, da die Nutzung der Cloud heute von der Mehrheit der Unternehmen genutzt wird und sie damit zu einem wachsenden Ziel für Angriffe wird. Hacker dringen in die "Cloud" der Unternehmen durch gestohlene Zugangsdaten eines Benutzers ein, was hauptsächlich auf die Verwendung schwacher Passwörter, gefolgt von gezielten Phishing-Angriffen und Verletzungen von Diensten Dritter zurückzuführen ist. Laut Microsoft (2017) haben die Angriffe auf Cloud-Benutzerkonten im ersten Quartal 2017 im Vergleich zum ersten Quartal 2016 um 300% zugenommen.

Nach den Ergebnissen derselben Studie ist Portugal das Land mit der größten Gefährdung durch Internetkriminalität auf Platz 8 und eines der Länder mit den meisten Opfern von Internetkriminalität in der EU (Platz 3).

Abbildung 9 - Cyber-Kriminalität - Sicherheitslückenbewertung

EU COUNTRY	CYBERCRIME VULNERABILITY SCORE				
1. MALTA (MOST VULNERABLE)	42%	11. SLOVENIA	38%	21. SWEDEN	32%
2. GREECE	41%	12. CROATIA	37%	22. ITALY	31%
3. ROMANIA	41%	13. DENMARK	36%	23. FRANCE	31%
4. SLOVAKIA	40%	14. LATVIA	35%	24. UK	31%
5. SPAIN	40%	15. CZECH REP	35%	25. NETHERLANDS	30%
6. LITHUANIA	39%	16. POLAND	34%	26. GERMANY	30%
7. CYPRUS	39%	17. IRELAND	33%	27. ESTONIA	30%
8. PORTUGAL	39%	18. LUXEMBOURG	32%	28. FINLAND (LEAST VULNERABLE)	29%
9. HUNGARY	39%	19. AUSTRIA	32%		
10. BULGARIA	38%	20. BELGIUM	32%		

Quelle: Website Builder Expert (2017)

Abbildung 10 – Quote der Cyberkriminalitätsopfer

Biggest Cybercrime victims in the EU

	% OF POPULATION WHO HAVE EXPERIENCED CYBERCRIME	ANNUAL AVERAGE MALWARE ENCOUNTER RATE	CYBERCRIME VICTIMHOOD RATING
1. ROMANIA	18%	28%	**23%**
2. NETHERLANDS	27%	14%	**21%**
3. PORTUGAL	15%	24%	**20%**
4. POLAND	16%	23%	**20%**
5. ITALY	17%	21%	**19%**

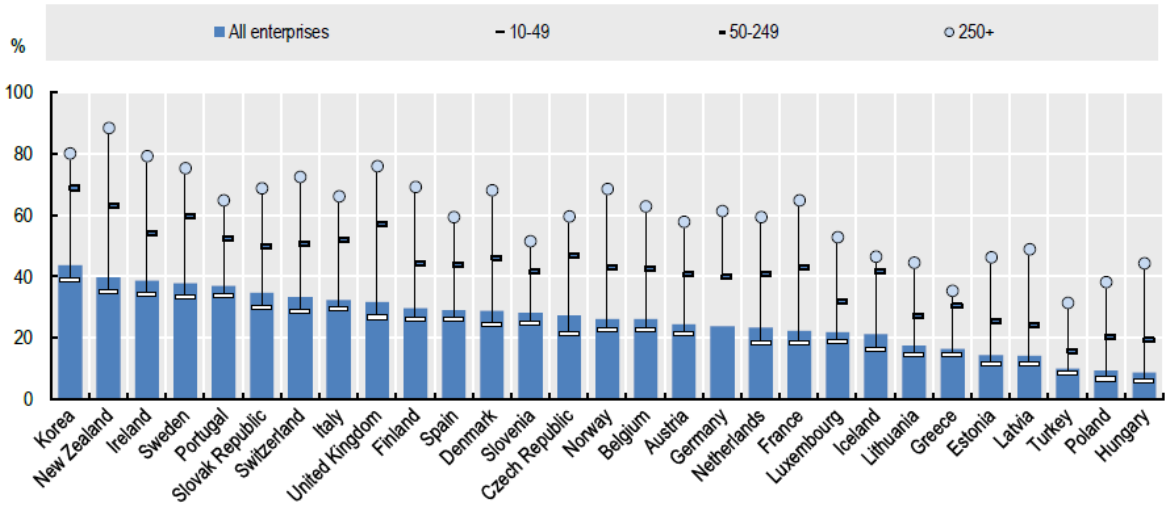
Quelle: Website Builder Expert (2017)

Es ist wichtig anzumerken, dass Portugal einen hohen Prozentsatz an Computern mit aktivierter Sicherheitssoftware hat, aber es gehört immer noch zu den Ländern, die anfälliger für Cybersicherheits-Kriminalität sind.

Was die Dimension der Unternehmen betrifft, so sind diejenigen mit 50 bis 249 Arbeitnehmern (47,1%) am stärksten betroffen, gefolgt von Unternehmen mit mehr als 250 Arbeitnehmern (42,6%), Unternehmen mit 10 bis 49 Arbeitnehmern sind diejenigen, die dieser Art von Vorfällen weniger ausgesetzt sind (OECD, 2017).

Wenn es um Unternehmen geht, die über eine formelle Politik zur Bewältigung ihrer Risiken im Bereich des digitalen Datenschutzes verfügen, ist Portugal eines der Länder, die in ihren Unternehmen mehr Richtlinien umgesetzt haben.

Abbildung 11 - Unternehmen, die über eine formelle Richtlinie zum Management von Risiken im Bereich des digitalen Datenschutzes verfügen (2015) (% aller Unternehmen)



Quelle: OECD (2017)

Zusammenfassend lässt sich sagen, dass das Risiko von Cybersicherheitsvorfällen in Portugal viel höher ist als im Durchschnitt der übrigen Unternehmen in der EU28.

Wenn es um die Datensicherheit geht, sind die größten Bedenken der portugiesischen Unternehmen:

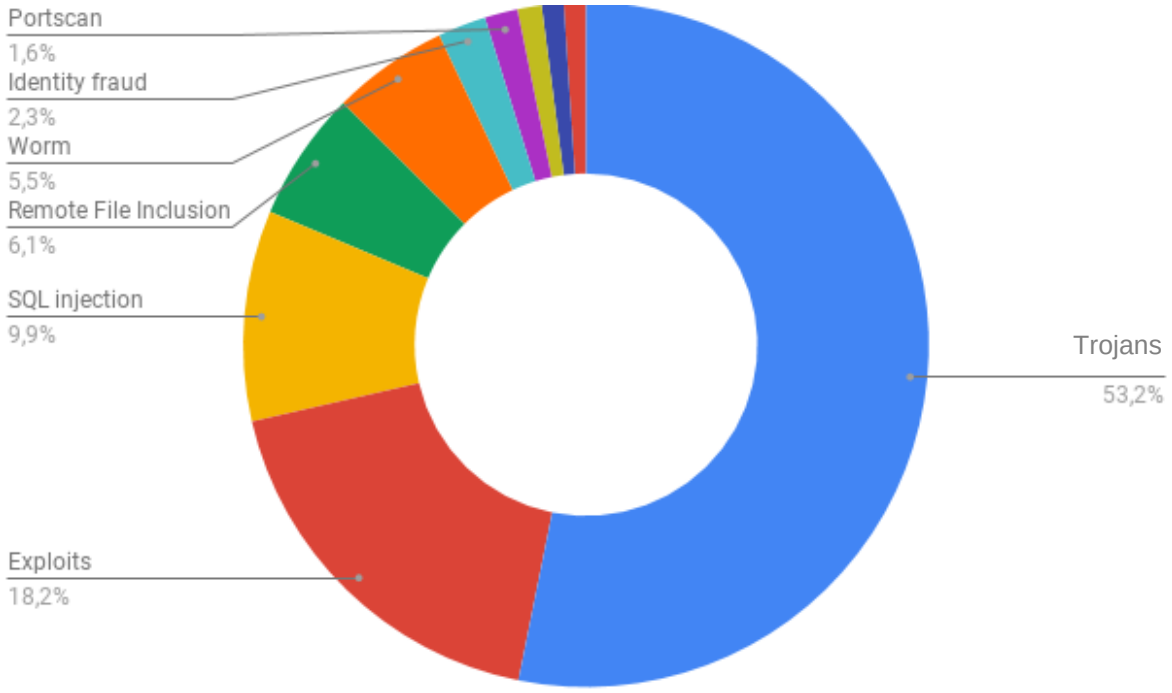
- **Internes Datenmanagement (61%),** wie z.B. die Risiken, die mit der Verantwortlichkeit für Datenverluste verbunden sind (59%),
- **Verstöße oder Cyber-Sicherheitsfehler** (43%)
- **Missbrauch von Daten beim Datenaustausch mit Partnern** (43%).

3.1.4. Spanien

Wie wir in der Abbildung unten sehen können, sind die häufigsten Angriffe in Spanien:

- Trojaner;
- Exploits und SQL Injektion.

Abbildung 12 – Häufigste Vorfälle



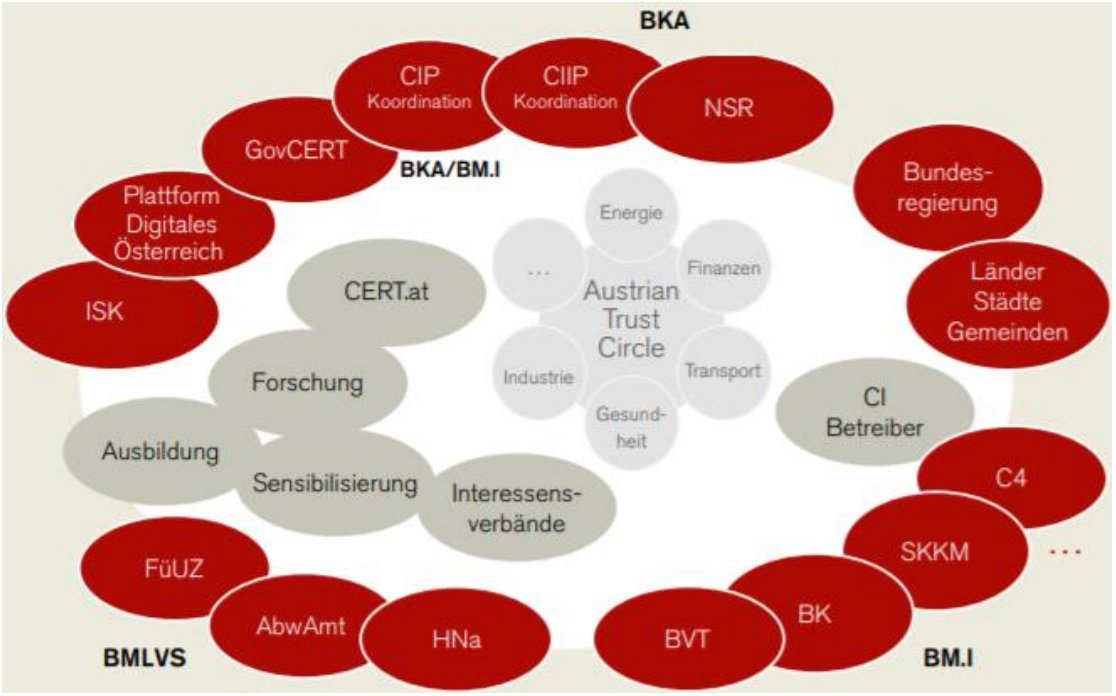
Quelle: Eigene Ausarbeitung des Autors (ccn-cert.cni, n.d.)

3.2. Gibt es in Ihrem Land Teams zur Überwachung der Internet- und Cybersicherheit von Unternehmen?

3.2.1. Österreich

Im Bereich des Cyberspace gibt es viele österreichische Strukturen und Interessenvertreter, die sich mit der Cybersicherheit auf einer sehr verteilten Basis beschäftigen. Mehrere Organisationen, die ausschließlich im Bereich der Cybersicherheit tätig sind, spielen in Österreich bereits eine wichtige Rolle, wie etwa die etablierten CERTs.

Abbildung 13 - Interessenvertreter in Österreich bei Cyber-Angriffen



Quelle: (Bundeskanzleramt, Digitales Österreich, 2012)

CERT.at ist das nationale österreichische Computer Emergency Response Team (Notfallteams), das 2008 gemeinsam mit GovCERT Austria vom Bundeskanzleramt (BKA) in Zusammenarbeit mit der österreichischen Domainregistrierungsstelle nic.at als Projekt bei nic.at eingerichtet wurde. CERT.at ist damit Ansprechpartner für IT-Sicherheit im nationalen Umfeld und ist für alle Fälle zuständig, die nicht durch ein spezifischeres CERT abgedeckt sind. CERT.at vernetzt andere Computer Emergency Response Teams (Notfallteams) und Computer Security Incident Response Teams (Reaktionsteam für Computersicherheitsverletzungen) aus den Bereichen kritische Infrastruktur und Informations- und Kommunikationstechnologie (IKT) und gibt Warnungen, Hinweise auf konkrete Fälle und Lösungen für Unternehmen und Privatpersonen.

GovCERT Austria ist das Government Computer Emergency Response Team für den öffentlichen Verwaltungssektor in Österreich. Es dient somit als primäre Anlaufstelle auf nationaler Ebene für die einzelnen Organe der öffentlichen Verwaltung im Falle eines Cyber-Angriffs.

Auf internationaler Ebene fungiert GovCERT Austria als österreichische Kontaktstelle für

ausländische Regierungen und internationale Organisationen in Fragen der IKT-Sicherheit. Es tauscht mit ihnen Informationen und Warnungen aus und leitet diese gegebenenfalls an inländische Interessenten weiter (Nic.at GmbH, 2018).

CERT.at und GovCERT unterstützen im Rahmen ihrer Möglichkeiten und Vorgaben bei Sicherheitsvorfällen. Während sich diese Unterstützung in den meisten Fällen auf die Bereitstellung von Informationen wie technische Hinweise oder Hinweise auf kommerzielle Anbieter für Internet Service Provider oder Domaininhaber beschränkt, fungieren CERT.at und GovCERT bei größeren Vorfällen als Koordinationsstelle und Schnittstelle zwischen den Betroffenen und anderen relevanten Akteuren auf nationaler und internationaler Ebene. Sie geben auch Handlungsanweisungen und tauschen Informationen darüber aus, wie Bedrohungen beseitigt werden können (Nic.at GmbH, 2018).

CERT.at muss nicht nur die Sicherheit im Internet in Österreich gewährleisten, sondern auch die Sicherheit der eigenen IT-Systeme und Infrastruktur ist ein entscheidender Faktor.

Eine Zertifizierung nach ISO 27 001/2017 ist der Nachweis, dass die IT-Sicherheit in einem Unternehmen umfassend und neben der Prüfung der Sicherheit der technischen Systeme und der Sicherheit der physischen Infrastruktur auch organisatorische Aspekte berücksichtigt werden. Die ISO 27 001-Zertifizierung ist ein Qualitätssiegel nach außen und andererseits auch ein ständiger Ansporn, die eigene innere Sicherheit zu gewährleisten. Jährliche Audits bei CERT.at stellen sicher, dass dieser Standard eingehalten wird (Nic.at GmbH, 2018).

Die wichtigsten CERTs in Österreich sind: A1-CERT; ACOnet-CERT; Austrian Energy CERT; BRZ-CERT; CERT.at; CERT-Verbund Österreich; GovCERT Austria; MilCERT; Raiffeisen Informatik CERT; sCERT; SV-CERT; TSA CERT; WienCERT; WILICERT.

3.2.2. Tschechien

In der Tschechischen Republik gibt es viele Organisationen, die sich aktiv am Schutz des Cyberspace beteiligen. Beispiele sind CERT oder das Computer Security Incident Response Team (CSIRT.CZ). CERTs sind in den vorherrschenden Computersicherheitsorganisationen und in verschiedenen globalen Sektoren der Regierung, des Handels und der Wissenschaft zu finden. Sie befassen sich mit technischen Fragen der Cybersicherheit, einschließlich der Lösung von Sicherheitsvorfällen von Personen, die wichtige Kommunikations- und

Informationssysteme für die Regierung verwalten, die Malware-Analyse, Sammlung und Auswertung von Informationen über Cyberattacken und Bedrohungen usw. CERT.CZ erfüllt Aufgaben wie die Gewährleistung der Verhinderung von Cyber-Bedrohungen und Angriffen gegen wichtige Betreiber von Informationsinfrastrukturen und Behörden sowie die Gewährleistung und die Koordinierung von Lösungen bei Cyber-Sicherheitsvorfällen von wichtigen Betreibern von Informationsinfrastrukturen und Behörden.

CSIRTs sind in der Regel Dienste, die für den Empfang, die Überprüfung und die Reaktion auf Berichte und Aktivitäten zu Computersicherheitsvorfällen verantwortlich sind. Ihre Dienste werden in der Regel für einen bestimmten Kundenkreis erbracht, der von einem Unternehmen bis zu einem zahlenden Kunden variieren kann.

In der Tschechischen Republik wurde das Tschechische Institut für Informatik, Robotik und Kybernetik (IDSA) gegründet, um eine einheitliche Umgebung für den Datenaustausch zwischen Benutzern in verschiedenen Industrie- und Produktionsumgebungen zu schaffen. Das Ziel von IDSA ist die Schaffung eines Ökosystems für den sicheren Datenaustausch, das auf einem einheitlichen Datenaustauschstandard zwischen internationalen Geschäftspartnern aufbaut.

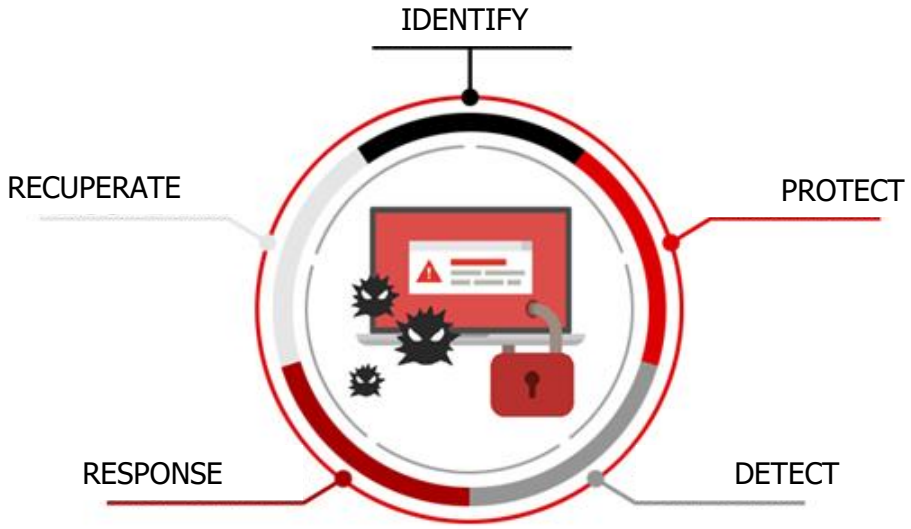
3.2.3. Portugal

In Portugal gibt es private Unternehmen und einen CNCS, die portugiesischen Unternehmen mit Cybersicherheitsproblemen mit einigen Dienstleistungen/Lösungen dabei unterstützen, ein verantwortungsbewussteres Verhalten und eine verantwortungsvollere Haltung im Internet zu entwickeln.

Wenn es um private Unternehmen geht, gibt es einige Dienstleistungen zum Online-Schutz, die meist von Versicherungs- und Sicherheitsfirmen angeboten werden. Einige dieser Lösungen umfassen Dienste, die den gesamten Lebenszyklus der Cybersicherheit analysieren. In der nächsten Abbildung sehen wir ein Beispiel für eine Dienstleistung, die von einer Technologiegruppe angeboten wird.

Der Dienst ist in fünf Stufen unterteilt: 1) Identifizieren (identify); 2) Schützen (protect); 3) Erkennen (detect); 4) Reagieren (response); und 5) Wiederherstellen (recuperate).

Abbildung 14 - Cyber-Sicherheitsdienste/-lösungen



Source: Gmv (n.d.)

In Portugal gibt es auch das CERT.PT, das ein integraler Bestandteil des CNCS ist und die Reaktion auf Vorfälle koordiniert, an denen staatliche Stellen, Betreiber von wesentlichen Diensten, Betreiber kritischer Infrastrukturen und Anbieter digitaler Dienste beteiligt sind. Über diesen Dienst koordiniert das CNCS die Reaktion auf Vorfälle im Bereich der Cybersicherheit, an denen staatliche Stellen, Betreiber wesentlicher Dienste und Anbieter digitaler Dienste, Betreiber kritischer nationaler Infrastrukturen und andere nationale Reaktionsteams für Computersicherheitsvorfälle beteiligt sind.

Die Komplexität und Transnationalität einer großen Anzahl von Cybersicherheitsvorfällen erfordert eine aggregierte Betrachtung und koordinierte Maßnahmen zwischen den verschiedenen beteiligten Stellen.

Außerdem sind private Sicherheitsunternehmen in Portugal aktiver, wenn es um die Präsentation von Dienstleistungen im Zusammenhang mit digitaler Sicherheit und verwalteten Sicherheitsdiensten auf dem Markt geht. Dennoch ist die Mehrheit der Organisationen dort noch immer nicht mit dem Schutz und der Sicherheit als integriertem Teil ihrer Strategie konfrontiert.

3.2.4. Spanien

2018 wurden in Spanien zwei neue technische Sicherheitsanweisungen veröffentlicht:

- Beschluss des Staatssekretärs für den öffentlichen Dienst vom 27. März 2018 zur Genehmigung der technischen Anweisung über Sicherheitsaudits für die Sicherheit von Informationssystemen;
- Beschluss des Staatssekretärs des öffentlichen Dienstes vom 13. April 2018 zur Genehmigung der technischen Sicherheitsanweisung für die Meldung von Sicherheitsvorfällen.

Beide kommen in Übereinstimmung mit dem National Security Framework (ENS) (Nationaler Sicherheitsrahmen) und dem zuvor veröffentlichten Sicherheitsstatusbericht zum ITS hinzu. Andererseits wird der Umsetzungsprozess für die Richtlinie (EU) 2016/1148 vom 6. Juli, die NIS-Richtlinie, die auch den öffentlichen Sektor betreffen wird, abgeschlossen, was unter anderem:

- die wesentlichen Dienstbetreiber ermitteln wird.
- die anzuwendenden Sicherheitsmaßnahmen.
- die zuständigen Behörden.
- die Referenz-CSIRTs festlegen wird.
- dem CCN-CERT die Koordinierung und die technische Reaktion in besonders schweren Fällen übertragen wird.

Darüber hinaus wurde als Ergebnis der vollständigen Anwendung der Verordnung (EU) 2016/679 vom 27. April 2016/679 über die Verarbeitung und den freien Verkehr personenbezogener Daten (DSGVO) ein neuer Entwurf für ein Organgesetz über den Datenschutz ausgearbeitet, der unter Aufhebung des geltenden Gesetzes alle Fragen regelt, die die allgemeine Datenschutzverordnung der Kommission überlässt.

Ccn-cert, das die verschiedenen Aktivitäten des nationalen Kryptologie- Zentrums begleitet, hat Folgendes entwickelt:

- ATHENEA ist das neue Schulungsinstrument für die Herausforderung der Cybersicherheit, das das Bewusstsein für die Bedeutung dieses Bereichs schärfen soll.

- GLORIA ist eine Plattform, die von alternden Cybersicherheitsvorfälle und -bedrohungen ausgeht und mit der auch die Carmen-, Lucía- und Reyes-Tools interoperabel sind, um die Erkennung, Analyse und den Austausch von Vorfällen zu erleichtern.
- SAT_ICS- Die Hauptfunktion des Frühwarnsystems für industrielle Steuerungssysteme ist die Früherkennung von Sicherheitsvorfällen. Es ermöglicht auch den Zugriff auf eine größere Anzahl von Erkennungsregeln und die Korrelation von Ereignissen, was die Unterstützung der Lösung von Vorfällen begünstigt.

3.3. Was tun diese Teams, wenn sie mit einem Cybersicherheitsvorfall in Bezug auf Unternehmen konfrontiert werden?

3.3.1. Österreich

Im Fall der IT-Sicherheit für KMUs können sie den IT-safe-Online-Leitfaden nutzen, um die Sicherheit ihrer eigenen IT-Infrastruktur zu bewerten. Das IT-Sicherheitshandbuch für KMUs bietet praktische Informationen über mögliche Gefahren und die richtigen technischen Maßnahmen, um diesen zu begegnen. In diesem Handbuch finden wir folgende Inhalte: Risikomanagement, Einhaltung gesetzlicher Vorgaben, IT-strategische Überlegungen, personelle Maßnahmen, Computersicherheit und Virenschutz, Netzwerksicherheit, Datensicherung und Notfallvorsorge, Bau- und Infrastrukturmaßnahmen, Expertengruppe IT-Sicherheit und Polizei - Kriminalprävention.

Abbildung 15 – IT-Sicherheitshandbuch

Quelle: (WKO Bundessparte Information und Consulting, 2019)

Im Fall der EPU-Checkliste für Ein-Personen-Unternehmen kann man in wenigen Minuten feststellen, ob und wo es Sicherheitsprobleme im IT-Bereich geben könnte. In einem Notfall (z.B. bei einem Cyber-Angriff oder bei der Verschlüsselung Ihrer Daten durch einen Erpressungstrojaner) leistet die Cybersiciherheits- Hotline unter 0800 888 133 rund um die Uhr kostenlose Hilfe.

Die Cybersicherheitshotline ist ein dreistufiges System:

1) Das Callcenter bietet 24 Stunden/Tag, 7 Tage die Woche unter der Nummer 0800 888 133 (kostenlos für Mitglieder) erste telefonische Informationen und Notfallhilfe;

2) Das Callcenter bietet einfache Erstmaßnahmen etc. an, aber weder technische Ferndiagnosen, noch Rechtshilfe oder Fragen zur Prävention, koordiniert (kostenlos für Mitglieder) aber gerne - falls notwendig und gewünscht - die Kontaktaufnahme zu

einem auf IT-Sicherheit und Cyberkriminalität spezialisierten Unternehmen der UBIT-Expertengruppe IT-Sicherheit aus Ihrer Nähe. Es empfiehlt sich, diese kostenlose Erstberatung mit dem IT-Sicherheitsunternehmen zu nutzen;

3) Das IT-Sicherheitsunternehmen kontaktiert die Geschädigten und führt ein kostenloses Erstgespräch auf der Grundlage der vom Call-Center erhobenen Daten durch. Obwohl Ferndiagnosen nie ein vollständiges Bild vermitteln können, können diese Spezialisten ihre Situation besser einschätzen und gegebenenfalls Informationen über konkretere Sofortmaßnahmen und Bewältigungsmaßnahmen für die Einrichtung des Normalbetriebs geben. Zudem hilft es zu ermitteln, ob und in welcher Form das IT-Sicherheitsunternehmen bei einem möglichen, über die Erstberatung hinausgehenden und kostenpflichtigen Vor-Ort-Einsatz helfen kann. Jeder weitere Einsatz muss dann direkt mit dem IT-Sicherheitsunternehmen vereinbart werden; die Kosten (Stundensatz etc.) für weitere Aktivitäten sind ebenfalls direkt mit dem IT-Sicherheitsunternehmen zu vereinbaren.

3.3.2. Tschechien

In der Tschechischen Republik gibt es viele Organisationen, die sich aktiv am Schutz des Cyberspace beteiligen. Beispiele sind CERT oder CSIRT.CZ.

CERTs sind in vielen Computersicherheitsorganisationen und verschiedenen globalen Sektoren der Regierung, des Handels und der Wissenschaft zu finden. Sie befassen sich mit technischen Fragen der Cybersicherheit, einschließlich der Lösung von Sicherheitsvorfällen von Personen, die wichtige Kommunikations- und Informationssysteme für die Regierung verwalten, die Malware-Analyse, Sammlung und Auswertung von Informationen über Cyberattacken und Bedrohungen und so weiter. CERT.CZ erfüllt Aufgaben wie die Gewährleistung der Verhinderung von Cyber-Bedrohungen und Angriffen gegen wichtige Betreiber von Informationsinfrastrukturen und Behörden sowie die Gewährleistung und Koordinierung von Lösungen bei Cyber-Sicherheitsvorfällen von wichtigen Betreibern von Informationsinfrastrukturen und Behörden.

CSIRTs sind in der Regel Dienste, die für den Empfang, die Überprüfung und die Reaktion auf Berichte und Aktivitäten zu Computersicherheitsvorfällen verantwortlich sind. Ihre Dienste

werden in der Regel für einen bestimmten Kundenkreis erbracht, der von einem Unternehmen bis zu einem zahlenden Kunden variieren kann.

In der Tschechischen Republik wurde die IDSA eingerichtet, um eine einheitliche Umgebung für den Datenaustausch zwischen Benutzern in verschiedenen Industrie- und Produktionsumgebungen zu schaffen. Das Hauptziel dieses Instituts ist die Schaffung eines Ökosystems für den sicheren Datenaustausch, das auf einem einheitlichen Datenaustauschstandard zwischen internationalen Geschäftspartnern aufbaut.

3.3.3. Portugal

Im Falle Portugals fungiert der CNCS als operativer Koordinator und nationale Behörde, die auf Cybersicherheit spezialisiert ist, zusammen mit den Einrichtungen der Betreiber der nationalen kritischen Infrastrukturen. Mit anderen Worten, der CNCS fördert die Nutzung des Cyberspace auf eine freie, zuverlässige und sichere Weise durch die kontinuierliche Verbesserung der nationalen Cybersicherheit und der internationalen Zusammenarbeit. Die Rolle dieser Institution besteht darin, nicht nur öffentliche Einrichtungen und kritische Infrastrukturen, sondern auch Unternehmen und die Zivilgesellschaft zu informieren und zu sensibilisieren. Andererseits ist es wichtig, dass das Land mit qualifizierten Ressourcen ausgestattet wird, um mit qualifizierten Arbeitskräften die komplexen Herausforderungen der Sicherheit im Cyberspace zu bewältigen.

Diese Institution spielt daher eine entscheidende Rolle in diesem Bereich in Portugal und ist dafür verantwortlich, verschiedene Arten von Hilfsmitteln zu organisieren und bereitzustellen, um eine Sicherheitskultur zu verbreiten, die allen das Wissen, das Bewusstsein und das Vertrauen vermittelt, die für die Nutzung von Informationssystemen erforderlich sind, um die Risiken des Cyberspace zu verringern.

Die Aufgabe des CNCS besteht darin, Maßnahmen und Instrumente zu implementieren, die notwendig sind, um Situationen zu prognostizieren, zu erkennen, zu reagieren und zu beheben, die aufgrund des bevorstehenden oder eingetretenen Auftretens von Zwischenfällen oder Cyber-Angriffen das Funktionieren staatlicher Behörden, kritischer Infrastrukturen und nationaler Interessen gefährden können.

Die Teams, die in diesen Organisationen arbeiten, organisieren:

- **Veranstaltungen** wie die C-DAYS, eine nationale Referenzveranstaltung mit Fokus auf große Themen im Zusammenhang mit Informationssicherheit und Cyberspace im Mittelpunkt. Diese Veranstaltung findet jedes Jahr statt und hat mehrere beteiligte Akteure (Industrie, Gesellschaft, Regierung, Industrie, Akademie,...);
- **Bewusstseins- Sitzungen zu verschiedenen Themen** der Cybersicherheit, die auf der Website des CNCS zu sehen sind;
- **Seminare,** bezeichnet als "Cibertemas", die sich auf Cybersicherheit beziehen und auch die Förderung von Projekten, Debatten und den Austausch von Ideen fördern.
- **Bewusstseinsbildung und Schulungsprogramm zu Cybersicherheit** in verschiedenen Teilen des Landes, vom Norden bis zum Süden, auf der Durchreise durch die Insel, mit Unterstützung der Partner;
- Die **Möglichkeit, bei einem eventuellen Zwischenfall zu benachrichtigen und Hilfe zu erhalten**;
- **Allgemeine Kurse** zur Cybersicherheit, die zwei Tage dauern. Die meisten dieser Arten von Veranstaltungen sind kostenlos, erfordern jedoch eine Anmeldung.

Wie bereits erwähnt, ist CERT.PT ein integraler Bestandteil des CNCS, der die Reaktion auf Vorfälle koordiniert, an denen staatliche Stellen, Betreiber von wesentlichen Diensten, Betreiber kritischer Infrastrukturen und Anbieter digitaler Dienste beteiligt sind. Die Koordination der Reaktion auf Vorfälle umfasst:

- die Durchsicht von Vorfallberichten, ihre technische und forensische Analyse;
- die Abstimmung mit den beteiligten nationalen und internationalen Stellen;
- die Koordinierung der Reaktion auf Vorfälle kann durch den CNCS beispielsweise bei einem Vorfall großen Ausmaßes eingeleitet oder über dafür vorgesehene Kanäle angefordert werden.

Im Bedarfsfall koordiniert der CNCS sein Vorgehen mit anderen nationalen Behörden. Dieser Dienst kann über die Website des CNCS, per E-Mail oder telefonisch angefordert werden.
Die Unternehmen, die mit einem Vorfall im Bereich der Cybersicherheit konfrontiert sind und eine gewisse Unterstützung insbesondere von Sicherheits- und Versicherungsgesellschaften

erhalten, sind besser geschützt und können ihre Probleme im Bereich der Cybersicherheit leichter lösen, da sie auf ein spezialisiertes Team zurückgreifen können, das weiß, was zu tun ist und wie Cybersicherheitsprobleme gelöst werden können. Jedes Unternehmen, das Dienstleistungen/Lösungen in diesem Bereich anbietet, hat seine eigenen Methoden, Werkzeuge, Kontrollen, Analysen, Tests und jeder Fall ist speziell.

3.3.4. Spanien

Die Cybersicherheitswelt ist äußerst dynamisch. Immer wieder tauchen neue Bedrohungen auf und es werden neue Schwachstellen entdeckt, auch wenn sie noch vor kurzem nicht als solche betrachtet wurden. Diese Tatsachen haben dazu geführt, dass sich die IT- und Netzwerkkommunikationssysteme weiterentwickeln, um diesen alarmierenden Umständen zu begegnen. Aus diesem Grund gibt es einen zunehmenden Bedarf an neuen Systemen zur Erkennung und Bewältigung von Sicherheitsvorfällen, die sich in Industrieanlagen auswirken könnten. Jeder erfasste Cybersicherheitsvorfall ermöglicht es, die Schwachstellen des Systems zu identifizieren und den Managementprozess darauf zu optimieren. Folglich sind die Erfahrungen, die die Teams in den CERTs einbringen, sehr wertvoll.

Eine der ersten Herausforderungen, die es zu bewältigen gilt, sind die Unannehmlichkeiten und Auswirkungen, die Sicherheitsmaßnahmen im täglichen Betrieb haben können. Dies ist besonders relevant, wenn eine Notfallreaktion erforderlich ist. Wenn es in diesem Fall zu einer Verzögerung kommt, die durch die angewandten Sicherheitsmaßnahmen verursacht wird, könnte das Ergebnis katastrophal sein. Darüber hinaus entwickeln sich die Techniken der Cyberangriffe ständig weiter. Diese Tatsache verlangt von den Betreibern der Einrichtungen, dass sie technisch auf dem neuesten Stand sind, auch wenn solche Herausforderungen nicht direkt mit ihrer Arbeit verbunden sind. Daher sollten neue automatische Reaktionsverfahren entwickelt werden, um Cybersicherheitsvorfälle zu erkennen und zu verhindern. Dennoch gibt es eine zusätzliche Schwierigkeit, Echtzeit-Betriebssysteme verfügen nur über eine begrenzte Kapazität zur Registrierung und Speicherung von Daten über die Situation vor und nach einer Bedrohung, wodurch die forensischen Beweise bei einem Vorfall reduziert werden. Die Verwaltung jedes einzelnen Vorfalls kann äußerst nützlich sein, um zukünftige Ereignisse zu verhindern, in kürzerer Zeit darauf zu reagieren und ihre Auswirkungen effizienter zu

verwalten. In Anbetracht all dessen müssen neue Instrumente und Verfahren zur Gewinnung und Nutzung dieses Wissens eingeführt werden, und zwar so, dass die beteiligten Unternehmen durch eine solche Tatsache nicht geschädigt werden.

Die Rolle und Erfahrung des CERT in Spanien ist aufgrund des bereits erworbenen Wissens und der Fähigkeiten, die in diesem neuen Umfeld angewandt werden können, ein Schlüssel für die Entwicklung dieses Punktes und für die Unterstützung der Entwicklung von Instrumenten, um:

- den Vorfall zu erkennen;
- seine Relevanz und seinen Umfang zu bewerten;
- über den Vorfall selbst zu berichten;
- die Kommunikation zwischen allen beteiligten Stellen zu ermöglichen;
- die Wiederherstellung implizierter Systeme technisch zu unterstützen;
- die Grundursache des Vorfalls zu identifizieren;
- zukünftige ähnliche Vorfälle zu vermeiden;
- Verbesserungen und eine Wissensbasis auf der Grundlage der gelernten Lektionen zu entwickeln
- die forensische Untersuchung des Vorfalls zu unterstützen.

Diese Dienste müssen von anderen unterstützt werden, die auch den Rest der Initiativen unterstützen:

- Die Ankündigung und Berichterstattung über laufende Angriffe;
- Identifizierung neuer Schwachstellen, Untersuchung, Klassifizierung und Veröffentlichung;
- Empfehlung neuer Maßnahmen zur Verbesserung der allgemeinen Cybersicherheit;
- Entwicklung und Katalogisierung der für den allgemeinen Markt verfügbaren Cybersicherheitslösungen;
- Entwicklung forensischer Technologien und Kapazitäten.

3.4. Identifizierung der Hauptrisiken/-schwierigkeiten, denen Menschen bei ihrer täglichen Arbeit im Bereich der Cybersicherheit ausgesetzt sind

3.4.1. Österreich

Die Bewertung der Trends für 2018 ergab ein sehr breites Spektrum an Beobachtungen und Einschätzungen. Nach der Kategorisierung und Gruppierung lassen sich die am häufigsten zitierten Trendeinschätzungen wie folgt zusammenfassen:

- Die Gefahrensituation nimmt zu, **die Angriffe werden immer komplexer und häufiger**, und die Hauptmotivation für die Angriffe ist die Monetarisierung;
- **Cloud-Sicherheit wird zu einem kritischen Thema,** und es wird erwartet, dass Unternehmen zunehmend von Cloud-Anbietern abhängig werden;
- Das **Netz- und Informationssystemsicherheitsgesetz (NISG) und die grundlegende Datenschutzverordnung stellen erhebliche Anforderungen an die Unternehmen**;
- Die Bedeutung von **organisatorischen Maßnahmen (z.B. Risikomanagement)** wird in Zukunft gegenüber rein technischen Maßnahmen **zunehmen**;
- Man geht davon aus, dass man sich nicht vollständig vor Angriffen schützen kann, und es ist wichtig, Angriffe schnell zu erkennen und richtig zu reagieren;
- Auch die **Abhängigkeit der Unternehmen von Hard- und Softwareprodukten** stellt eine zunehmende Bedrohung dar.

3.4.2. Tschechien

Die Hauptbedrohungen, denen die Menschen bei der Arbeit am häufigsten ausgesetzt sind, sind:

- **Zunehmende Datenmengen (Big Data) und die Frage der Verwaltung und Sicherheit dieser Datenmengen.** Schutz und Datensicherheit sind für Tschechien sehr wichtig, insbesondere für diejenigen, die im öffentlichen Interesse liegen. Im öffentlichen und privaten Sektor wächst die Datenmenge, und es ist notwendig, weiterhin mehr Daten zu speichern. Deshalb begannen sie, neue Formen der Datenspeicherung zu nutzen, zum Beispiel Cloud- Speicher. Die verstärkte Nutzung

dieser Online-Dienste und der Cloud führt jedoch häufig zu intransparenten Sicherheitslösungen, deren Glaubwürdigkeit fragwürdig sein kann;

- **Vielfalt der mobilen Geräte ("Bringen Sie Ihr eigenes Gerät mit").** Eine bedeutende interne Bedrohung ist ein besorgniserregender Trend der wachsenden Akzeptanz der Vorgabe "bring dein eigenes Gerät mit". Mit der Vorgabe "bring dein eigenes Gerät mit" werden Zielfirmen zunächst die Geräte persönlicher Mitarbeiter infizieren, die keine strengen Sicherheitsmaßnahmen implementiert haben, und dann durch sie Trojaner einsetzen, die das Netzwerk infizieren. Die Richtlinien für die Verwendung von Hardware, die sich im Besitz von Mitarbeitern befindet, müssen gründlich geprüft und, falls erforderlich, aktualisiert und erweitert werden;
- **Sicherheit und Datenschutz von Cloud-Diensten.** Die Angriffe auf Cloud-Dienste nehmen an Stärke zu, und es wird erwartet, dass es in naher Zukunft zu einem großen Sicherheitsbruch in der Cloud kommen wird. Heutzutage dauern drei Viertel einer Sicherheitsverletzung Tage, Wochen oder sogar Monate, bevor sie entdeckt werden, und erhöhen somit den Schaden der Angreifer erheblich;
- **Notwendigkeit der Verfolgung der Datenbewegung innerhalb der Organisation.** Verhaltensanalyse-Technologien ermöglichen Unternehmen und Institutionen die Überwachung von Benutzern innerhalb von Unternehmen und Endbenutzern. Dies kann zu einer Warnung vor verdächtigem Verhalten führen, bei dem es sich um Datendiebstahl oder Angriffe durch schädliche Software handelt;
- **Angriffe, um zu zerstören.** Einige ideologisch profilierte Hacktivistengruppen behaupteten, dass sie weiterhin versuchen werden, zerstörerische Angriffe gegen die Interessen bestimmter Unternehmen oder öffentlicher Einrichtungen zu führen;
- **Sicherheitsrisiken im Zusammenhang mit der Computerisierung der öffentlichen Verwaltung (eGovernment).** Beispielsweise birgt der elektronische Beschaffungsprozess neue Risiken, die die Glaubwürdigkeit des Beschaffungsverfahrens und die Sicherheitsrisiken gefährden können, die mit der Tatsache verbunden sind, dass elektronische Beschaffungsinstrumente an das öffentliche Netzwerk angeschlossen sind.

Der beste Weg, um die angemessene Reaktion auf einen Zwischenfall in einer bestimmten Situation zu bestimmen, besteht darin, zu verstehen, welche Arten von Angriffen wahrscheinlich eingesetzt werden. Es gibt eine Liste der verschiedenen Angriffsvektoren, denen Menschen bei ihrer Arbeit im Bereich der Cybersicherheit ausgesetzt sind:

- **Externe/abnehmbare Geräte:** Ein Angriff, der von einem Wechseldatenträger (z.B. Flash-Laufwerk, CD) oder einem Peripheriegerät ausgeführt wird;
- **Email:** Ein Angriff, der über eine E-Mail-Nachricht oder einen Anhang ausgeführt wird (z.B. Malware-Infektion);
- **Verschleiß:** Ein Angriff, bei dem Brute-Force-Methoden (Exhaustionsmethode) eingesetzt werden, um Systeme, Netzwerke oder Dienste zu gefährden, zu verschlechtern oder zu zerstören;
- **Unsachgemäße Nutzung:** Jeder Vorfall, der aus der Verletzung der akzeptablen Nutzungsrichtlinien einer Organisation durch einen autorisierten Benutzer resultiert, mit Ausnahme der oben genannten Kategorien
- **Web:** Ein Angriff, der von einer Website oder einer webbasierten Anwendung aus ausgeführt wird (z.B. Drive-by-Download);
- **Verlust oder Diebstahl von Ausrüstung:** Der Verlust oder Diebstahl eines Computergeräts oder der von der Organisation verwendeten Medien, wie z.B. eines Laptops oder Smartphones.

3.4.3. Portugal

In Portugal sind die Hauptrisiken und Schwierigkeiten, denen Arbeitnehmer in ihrem Berufsleben ausgesetzt sind, folgende:

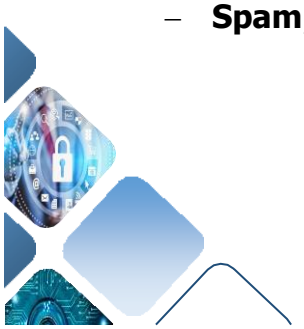
- **Web-Angriffe, deren Hauptmotivation die Monetarisierung und Verbreitung von vertraulichen/privaten Informationen ist**;
- **Phishing**;
- **Spam**;
- **Malware-Infektionen durch E-Mail;**
- **Web-basierte Angriffe;**;
- **Cloud- Sicherheit und Datenschutz**;

- **Datenschutzmanagement**;
- **Exposition gegenüber Informatik-Angriffen, Systemausfällen und Datenverletzungen**;
- **Globales Risikoprofil der Unternehmen** (einige Tätigkeitsbereiche sind stärker gefährdet als andere);
- **Mangelnde Kenntnisse zur Aufdeckung gefälschter Informationen**, die z.B. zu Infektionen und Datenraub führen können;
- Ein **Web-Angriff**, der von einer nicht vertrauenswürdigen Quelle ausgeführt wird;
- Die **zunehmende Nutzung von Hardware- und Softwareprodukten** stellt ebenfalls eine zunehmende Bedrohung dar.

3.4.4. Spanien

Die Hauptrisiken/-schwierigkeiten, denen die Spanier heutzutage ausgesetzt sind, sind:

- **Malware**;
- **Webbasierte Angriffe.** Da der Großteil der Geschäftsvorgänge online abgewickelt wird, sind webbasierte Angriffe im Zunehmen. Cyberkriminelle werden immer innovativer und nutzen ausgeklügelte Techniken, um ungepatchte Schwachstellen in den Webanwendungen auszunutzen. Das Motiv hinter diesen Angriffen kann ein anderes sein, nämlich der Diebstahl sensibler Informationen eines Unternehmens, die Anzeige von Spam-Werbung auf der Website oder das Herunterladen von Malware auf den Computer des Benutzers;
- **Angriffe auf Webanwendungen** werfen eine Reihe von Sicherheitsbedenken auf, die auf unsachgemäße Kodierung zurückzuführen sind. Schwerwiegende Schwächen oder Schwachstellen ermöglichen es Kriminellen, direkten und öffentlichen Zugang zu Datenbanken zu erhalten, um sensible Daten zu verbreiten. Viele dieser Datenbanken enthalten wertvolle Informationen (z.B. persönliche Daten und finanzielle Einzelheiten), die sie zu einem häufigen Ziel von Angriffen machen.;
- **Datenverletzungen;**
- **Phishing**;
- **Spam**;



- **Dienstverweigerung**;
- **Botnets**.

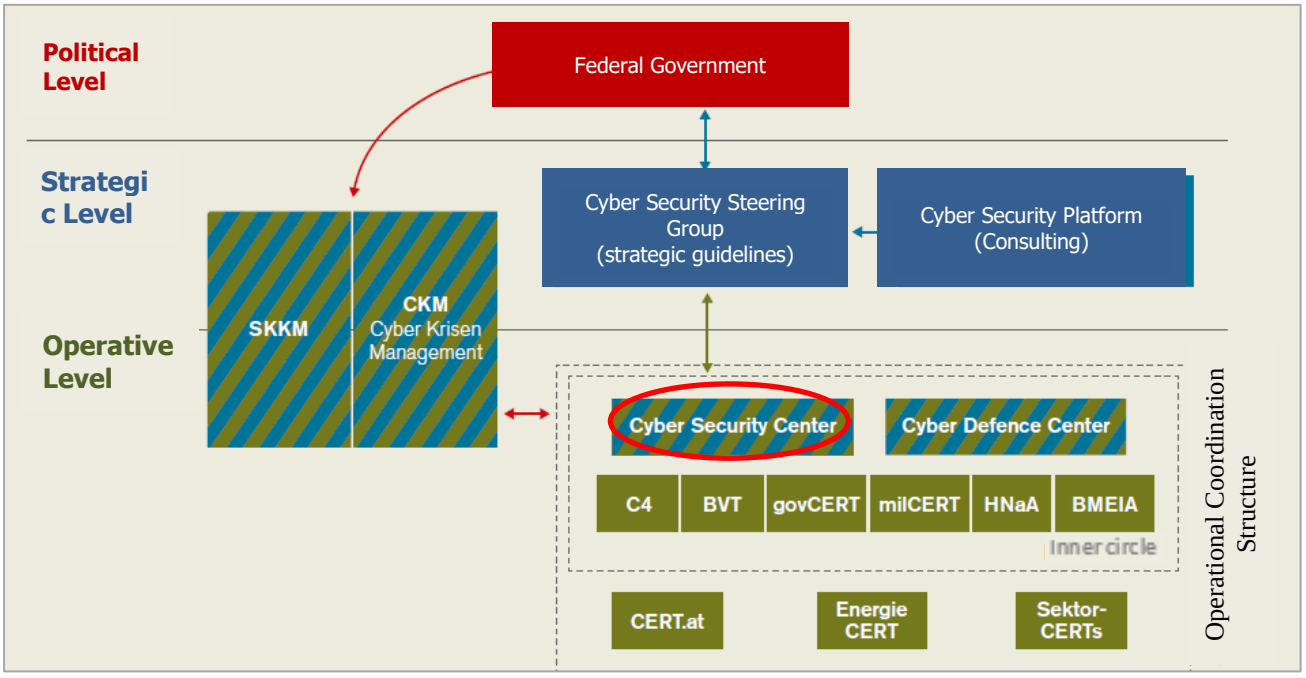
3.5. Was wird in Ihrem Land angewandt, um die Internetsicherheit der Bürger bei ihrer Arbeit zu verbessern?

3.5.1. Österreich

Zum Schutz des Cyberspace und der Menschen im virtuellen Raum sieht die Österreichische Strategie für Cybersicherheit - Österreichische Strategie für Cyber Sicherheit (ÖSCS) u.a. die Schaffung einer Struktur für die Koordination auf operativer Ebene vor. Auch die Strategie INNEN.SICHER nennt die Cybersicherheit als eine zentrale Herausforderung.

Als Ergebnis wurde das INNEN.SICHER-Projekt "Cyber Security. BVT" gestartet, dessen zentrales Element die Einrichtung eines CSC im Bundesministerium des Innern ist. Dieses Projekt wurde im Dezember 2017 mit der Überführung des CSC in den Regelbetrieb erfolgreich abgeschlossen. Die Bedeutung des Projekts wird unter anderem dadurch unterstrichen, dass die EU erhebliche Mittel aus dem Fonds für innere Sicherheit zur Verfügung gestellt hat.

Abbildung 16 – Cybersicherheit in Unternehmen



Quelle: (Cyber Sicherheit Steuerungsgruppe, 2018)

Die zentralen Aufgaben des CSC basieren auf vier Säulen: Behörde für Netz- und Informationssicherheit, Prävention und Schutz kritischer Infrastrukturen, Koordination und Cyber-Krisenmanagement sowie technische Kompetenz und Ansprechpartner.
Eine wesentliche zentrale Aufgabe ist die Durchführung einer umfassenden Präventionsarbeit durch:

- **Aufklärungsveranstaltungen;**
- **Vorträge;**
- **Beratungsgespräche;**
- **Gute Zusammenarbeit mit der Industrie und den bestehenden Strukturen** im Bereich der Cybersicherheit in Österreich.

Das IKT-Sicherheitsportal onlinesicherheit.gv.at ist eine Initiative in Zusammenarbeit mit der österreichischen Wirtschaft und fungiert als zentrales Internetportal für Themen rund um die Sicherheit in der digitalen Welt. Als strategische Maßnahme der nationalen IKT-Sicherheitsstrategie und der österreichischen Strategie für Cybersicherheit verfolgt die Initiative das Ziel, die IKT- und Cybersicherheitskultur in Österreich zu fördern und nachhaltig zu stärken, durch:

- **Sensibilisierung und Bewusstseinsbildung bei den betroffenen Zielgruppen** und durch zielgruppenspezifische Handlungsempfehlungen;
- **Das Informations- und Dienstleistungsangebot** wird im Rahmen regelmäßiger Redaktionssitzungen mit den 39 Kooperationspartnern (Bundesministerien, Landesregierungen, Behörden, Fachhochschulen, Forschungseinrichtungen, Unternehmen, Verbände und Interessengruppen) kontinuierlich ausgebaut. Es enthält aktuelle Nachrichten und Warnungen, Hinweise und weitere Informationen für Einsteiger und Experten;
- **Informationen durch Nachrichtenartikel, Publikationen und Veranstaltungseinträge.** Im Jahr 2018 wurde jeden Monat ein Schwerpunktthema zu aktuellen Trends definiert, zu dem insgesamt 34 Fachartikel veröffentlicht wurden;
- **Schulungsaktivitäten (Kurse);**
- **Vorbeugende Maßnahmen und intensive Ermittlungsarbeit;**

- **Verstärkte Präventionsarbeit und Polizeiprojekte wie "CyberKids" und "Click & Check"**.

3.5.2. Tschechien

Im Zuge der fortschreitenden Digitalisierung ist jedes Unternehmen natürlich weniger widerstandsfähig gegenüber virtuellen Sicherheitsrisiken. Experten in Tschechien haben fünf Cybersicherheitsregeln für Unternehmen definiert:

- **Die Unternehmen sollten ein spezielles Sicherheitsteam bilden und es in strategische Maßnahmen einbeziehen;**
- **Die Einbeziehung der Mitarbeiter zur Beteiligung** an den Ergebnissen kann einer der zuverlässigsten Schritte sein, die man unternehmen kann;
- **Kundenschutz.** Aufgrund der Vernetzung der Büros der Zukunft sollten Unternehmen ihren Kunden helfen zu verstehen, wie sie sich nicht nur vor rechtlichen Problemen schützen können. Organisationen sollten aktiv versuchen, die Auswirkungen sowohl neuer als auch künftiger Gesetze zu verstehen, damit sie ihre Kunden richtig beraten können;
- **Unternehmen sollten mit ihren Partnern, Lieferanten und anderen Dritten zusammenarbeiten,** um Wissen, Produkte und Dienstleistungen im Zusammenhang mit der Cybersicherheit auszutauschen;
- **Unternehmen sind selten bereit, Informationen zu teilen oder mit anderen zusammenzuarbeiten,** aber die Informationen, die sie über einen von ihnen erlittenen Cyber-Angriff geben können, sind sehr wichtig, damit mehrere Beteiligte wissen und darüber nachdenken, was sie tun können, um einen ähnlichen Cyber-Angriff zu vermeiden.

Heute ist ein gemeinsamer Teil der Unternehmensführung das Informationssicherheits-Managementsystem. Die grundlegenden Elemente, die in internen Unternehmensnetzwerkschutzsystemen verwendet werden, sind:

- **Virenschutz auf Arbeitsplatzebene**, zum Beispiel auf der Ebene von Internet-Gateways;

- **Antivirenschutz für Dateiserver und Groupware-Umgebungen;**
- **Antiviren-Schutz für die Kommunikation über Internet-Gateways;**
- **Schutz vor E-Mail-Spam;**
- **Systeme zur Erkennung und Verhinderung von Eindringlingen.** Dabei handelt es sich um ziemlich ausgefeilte Sicherheitswerkzeuge, die einen laufenden Angriff erkennen (IDS) und Maßnahmen zu dessen Beseitigung ergreifen können (IPS). Die Implementierung dieser Systeme ist länger und anspruchsvoller, was Administratoren oft davon abhält, sie konsequent zu nutzen.

3.5.3. Portugal

Die gängigsten guten Praktiken, die Menschen bei ihrer Arbeit anwenden, sind:

- **Teilnahme an Veranstaltungen** wie den C-DAYS, einer nationalen Referenzveranstaltung, die ein großes Thema im Zusammenhang mit Informationssicherheit und Cyberspace in den Mittelpunkt stellt;
- Verwendung von **Antiviren-Software in Computern;**
- Zugang zu **Informationen über Zeitschriften, Websites und die allgemeinen Medien**;
- **Sensibilisierungssitzungen zu verschiedenen Themen** der Cybersicherheit;
- **Seminare** im Zusammenhang mit der Cybersicherheit, die auch die Projektförderung, die Debatte und den Austausch von Ideen fördern;
- **Sensibilisierung und Teilnahme am Ausbildungsprogramm in Cybersicherheit** durch CNCS, das die Bildung und das Bewusstsein massiv verstärken soll;
- **Einsatz spezieller Sicherheitsteams,** die in der eigenen Firma (nicht so häufig) und durch ein auf Sicherheit spezialisiertes Unternehmen im Unterauftrag tätig sind;
- Die **Möglichkeit**, bei einem eventuellen Zwischenfall zu **benachrichtigen und Hilfe zu erhalten**;
- **Allgemeine Ausbildungsaktivitäten** (Kurse und Workshops), die nur einmal in gewisser Weise stattfinden;
- **Interne Schulung durch ein Teammitglied**.

3.5.4. Spanien

Um die Sicherheit zu verbessern, wird es in mehreren Bereichen umgesetzt, die im Folgenden beschrieben werden:

- **Beteiligung der Unternehmen an allen Initiativen** in der Weise, dass sie mit ihrer Erfahrung und ihrem Wissen dazu beitragen können;
- **Entwicklung von Programmen, Werkzeugen, Techniken und Referenzdokumenten, die die Leistung von Cybersicherheitsexperten unterstützen können.** Unter diesen Referenztechniken müssen Implementierungsmethoden, Cybersicherheitsrichtlinien und -verfahren sowie Leitfäden für bewährte Praktiken für jeden Industriesektor entwickelt werden.;
- **Organisation von Schulungsinitiativen, kostenlosen Handbüchern und Workshops,** die die unterschiedlichen Bedürfnisse aller damit verbundenen Rollen berücksichtigen. Besonderes Augenmerk sollte dabei auf die IT-Fachleute gelegt werden, die sich mit dem Schutz von Automatisierungsanlagen und Steuerungssystemen befassen wollen. Es muss der Ausbildungsbedarf der Fachleute und Steuerungsingenieure berücksichtigt werden, die die neuen Steuerungs- und Automatisierungsinfrastrukturen sicher gestalten wollen;
- **Veröffentlichung von ausführlichen Analyseberichten auf Führungsebene über die Vorteile der Cybersicherheit**;
- **Beaufsichtigung und ständige Überwachung der Meilensteine und Fortschritte, die sich auf die industrielle Cybersicherheit auswirken können,** um die Wirksamkeit der durchgeführten Maßnahmen zu gewährleisten.

In diesem Zusammenhang können wir die Entwicklung der Telefonica-Gruppe hervorheben, die zu Beginn des Jahrhunderts begann, die Linie der Cybersicherheit zu bilden und heute 16 CSIRTs hat, die über die ganze Welt verteilt sind. Darüber hinaus wird die zur BBVA-Gruppe gehörende Tochterfirma, die als Experte für Ingenieurwesen "Next" gilt, die technologische Transformation der BBVA-Bank vorantreiben. Zu diesem Zweck verfügt sie über fortschrittliche Experten für Massenanalyse und Makrodaten, KI, Blockchain und Cybersicherheit. Was die Cybersicherheit betrifft, so verfügen sie über ein zahlungskräftiges Team, das fortschrittliche

professionelle Sicherheitsdienste einschließlich Infrastruktur- und Anwendungslösungen, Entwicklung sicherer Software und Cybersicherheitslösungen sowohl für die BBVA-Gruppe als auch für führende Unternehmen anbieten wird.

4. Internetsicherheit und Industrie 4.0: im Privatleben

4.1. Welche Fälle der Internetsicherheit wurden in Ihrem Land in den letzten Jahren im Privatleben der Bürger gelöst?

4.1.1. Österreich

Für Österreich gab es keine Informationen zu diesem Thema.

4.1.2. Tschechien

Die häufigsten Angriffe im Privatleben der Bürger sind:

- **Virus:** Der häufigste Virus kann durch E-Mail- und SMS-Anhänge, das Herunterladen von Internet-Dateien und Betrugslinks in sozialen Medien verbreitet werden;
- **Wurm:** E-Mail-Würmer werden normalerweise durch das Erstellen und Senden von ausgehenden Nachrichten an alle Adressen in der Kontaktliste eines Benutzers verbreitet;
- **Betrug:** Einige der häufigsten Betrugsfälle sind: Phishing; Spendenbetrug (eine Person, die behauptet, ein Kind zu haben oder jemanden mit einer Krankheit zu kennen und die finanzielle Unterstützung benötigt); Catfish (eine Person, die ein gefälschtes Online-Profil mit der Absicht erstellt, jemanden zu täuschen); und Ketten-Mail, die normalerweise harmlos ist, über E-Mail verbreitet wird und die Leute dazu auffordert, die E-Mail weiterzuleiten;
- **Spam**: Die meisten E-Mail-Spam-Nachrichten sind kommerziell. Ob kommerziell oder nicht, viele sind nicht nur ärgerlich, sondern auch gefährlich, weil sie Links enthalten können, die zu Phishing-Websites oder Websites führen, die Malware hosten oder Malware als Dateianhänge enthalten;
- **Phishing**.

4.1.3. Portugal

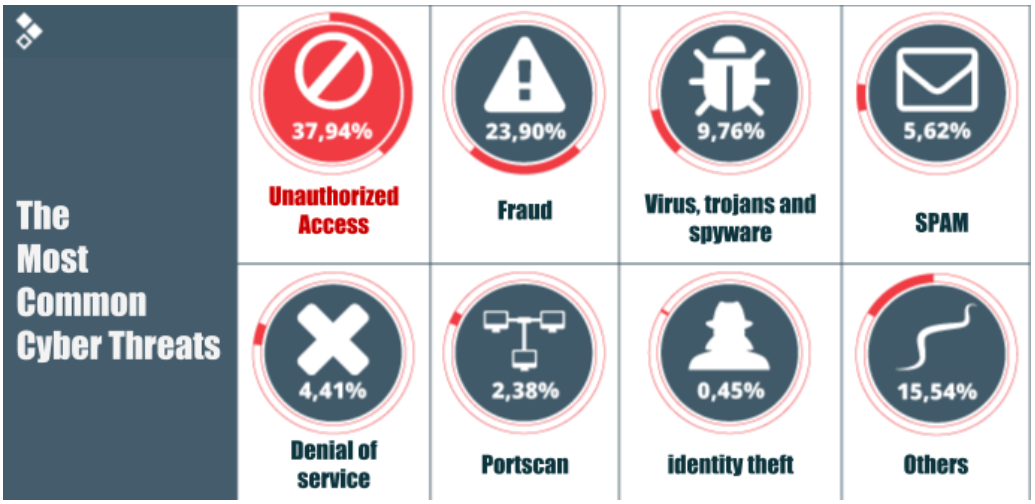
Die häufigsten Vorfälle, mit denen Menschen in ihrem Privatleben konfrontiert werden, sind:

- **Virus**;
- **Phishing**;
- **Spam**;
- **Unautorisierter Zugriff**;
- **Identitätsdiebstahl vor allem in sozialen Medien.**

4.1.4. Spanien

Die häufigsten Cyber-Angriffe, wie wir in der nächsten Abbildung sehen können, sind: unbefugter Zugang und Betrug.

Abbildung 17 – Häufigste Vorfälle



Quelle: (INCIBE, n.d.).

4.2. Gibt es in Ihrem Land Teams zur Überwachung der Internet- und Cybersicherheit der Bürger in ihrem Privatleben?

4.2.1. Österreich

In Österreich ist das Team, das für die Überwachung der Internet- und Cybersicherheit der Bürger verantwortlich ist, das Cyber Crime Competence Center (C4). Das Cyber Crime Competence Center (C4) ist die nationale und internationale Koordinations- und Meldestelle

für die Bekämpfung der Internetkriminalität. Das Zentrum setzt sich aus technisch und fachlich hoch spezialisierten Experten aus den Bereichen Ermittlung, Forensik und Technologie zusammen. Das Cyber Crime Competence Center C4 wurde 2011 zur Bekämpfung der Computerkriminalität als eigene Einheit innerhalb der Kriminalpolizei des Bundeskriminalamtes gegründet. Das Cyber Crime Competence Center C4 ist in vier Einheiten gegliedert: "Zentrale Aufgaben", "Sicherung von IT-Beweismitteln", "Ermittlungen", "Entwicklung und Innovation" und die Meldestelle.

Abbildung 18 - Logo Cyber Crime Competence Center (C4)

Quelle: (Bundeskriminalamt[1], 2019)

Die Meldestelle für Internet-Kriminalität (C4) ist einerseits die Anlaufstelle für die Bevölkerung. So können neue Phänomene frühzeitig erkannt werden. Andererseits ist sie auch die Schnittstelle zum CSC und eine internationale Kontaktstelle in Sachen Cyberkriminalität. Eine weitere wichtige Aufgabe ist die Kontaktstelle für alle Polizeidienste im Zusammenhang mit der Cyber-Kriminalität (Cyber Sicherheit Steuerungsgruppe, 2018).

4.2.2. Tschechien

Die Vereinigung NarodniCentrumBezpecnejsiholInternetu (NCBI) ist Mitglied des paneuropäischen Netzwerks nationaler Zentren für sicherere Bewusstseinsbildung INSAFE. In Zusammenarbeit mit seinen Partnern organisiert NCBI Konferenzen, Seminare, Vorträge und Schulungen zum Thema sicherere Internetnutzung und Internetkriminalitätsprävention in Tschechien.

Abbildung 19 - Logo NCBI

Quelle: (S@ferinternet.cz, n.d.)

Das Zentrum für die Prävention riskanter virtueller Kommunikation ist ein Institut, das sich mit riskanten Formen der Online-Kommunikation von Kindern und Erwachsenen befasst. Es konzentriert sich auf Cyberbullying, Cyberstalking, Hoaxes und Spamming, Sexting, Social Engineering in der Online-Gemeinschaft, das Risiko des Austauschs persönlicher Daten in sozialen Netzwerken und anderen gefährlichen Kommunikationsphänomenen.

4.2.3. Portugal

In Portugal gibt es einige wenige Institutionen, die der portugiesischen Gesellschaft helfen können, Vorfälle im Bereich der Internetsicherheit zu verhindern. Die Institutionen können wie folgt beschrieben werden:

In Portugal gibt es zwei Einrichtungen, die die Web-Sicherheit und den Schutz persönlicher Daten fördern:

- **CNPD:** Die erste und bekannteste ist die CNPD, die eine unabhängige Verwaltungseinheit mit Befugnissen ist, die mit der Versammlung der Republik zusammenarbeitet. Die CNPD arbeitet mit den Datenschutzaufsichtsbehörden anderer Staaten zusammen, insbesondere bei der Verteidigung und Ausübung der Rechte der im Ausland lebenden Personen. Des Weiteren ist die CNPD das Organ, das befugt ist, die Einhaltung der Gesetze und Vorschriften im Bereich des Schutzes personenbezogener Daten unter strikter Achtung der Menschenrechte und der Freiheit zu überwachen und zu kontrollieren. Die CNSC will Freiheit, Sicherheit und einen gerechten Cyberspace für alle garantieren. In kurzfristiger Sicht gibt dieses Konsortium einige Antworten, um unerwünschte Ereignisse zu verhindern. Mittel- bis langfristig ist es das Ziel, gute Praktiken im Bereich der Cybersicherheit zu entwickeln.

Abbildung 20 - Logo CNPD

Quelle: (CNPD, n.d.)

- **Vereinigung "Associação dos Profissionais de Proteção e de Segurança de Dados":** Dies ist eine Berufsvereinigung, die Einzelpersonen und Organisationen vertritt, und sich mit dem Schutz und der Datensicherheit, der Regulierung der Privatsphäre und der elektronischen Kommunikation befasst oder die die Position von Datenschutzbeauftragten in Organisationen innehat, die auf portugiesischem Gebiet tätig sind.

4.1.4. Spanien

INCIBE-CERT ist eines der Referenzteams für die Reaktion auf Vorfälle, die die Effizienz bei der Bekämpfung von Straftaten im Zusammenhang mit Netzwerken und Informationssystemen verbessern und deren Auswirkungen auf die öffentliche Sicherheit verringern. Die Aufgabe von INCIBE besteht darin, die Cybersicherheit, das Vertrauen und den Schutz der Privatsphäre in Bezug auf die in der Informationsgesellschaft angebotenen Dienste zu stärken und der Öffentlichkeit, den Unternehmen, der spanischen Regierung, dem spanischen Hochschul- und Forschungsnetz, dem Informationstechnologiesektor und strategischen Sektoren im Allgemeinen einen Mehrwert zu bieten.

INCIBE ist das Referenzzentrum für die Reaktion auf Sicherheitsvorfälle für Bürger und privatrechtliche Körperschaften in Spanien, das vom Spanischen Nationalen Institut für Computersicherheit betrieben wird und dem Ministerium für Wirtschaft und Unternehmen über den Staatssekretär für digitale Förderung untersteht. Als Exzellenzzentrum ist INCIBE eine Dienstleistung der spanischen Regierung, die auf die Entwicklung der Cybersicherheit als Instrument für die soziale Transformation und die Entwicklung neuer Innovationsfelder

hinarbeitet. Zu diesem Zweck leitet INCIBE mit seinen Aktivitäten, die sich auf die Forschung, die Bereitstellung von Dienstleistungen und die Zusammenarbeit mit den relevanten Akteuren konzentrieren, eine Reihe von Initiativen, die auf nationaler und internationaler Ebene auf Cybersicherheit ausgerichtet sind.

Abbildung 21 - Logo incibe

Quelle: (Incibe.es, n.d.)

4.3. Was tun Bürger in Ihrem Land, wenn sie mit einem Cybersicherheitsvorfall konfrontiert werden?

4.3.1. Österreich

In Österreich gibt es verschiedene und themenspezifische Hotlines, an die Sie sich wenden können, wenn Sie Opfer einer IT-Kriminalität geworden sind. Je nach Art des Cybersicherheitsvorfalls kann man sich auf unterschiedliche Behörden verlassen. Es gibt auch einige Institutionen, die wichtige Informationen (z.B. Tipps) zur Vermeidung von Cybersicherheitsvorfällen zur Verfügung stellen.

- **Die Watchlist Internet**: Diese Institution listet auf ihrer Website zahlreiche Artikel über verschiedene Betrugsversuche, wie z.B. Fake-Shops, Phishing, gefälschte Rechnungen und Abonnementfallen auf. Dies ist auch eine Liste von betrügerischen Online-Shops, die immer auf dem neuesten Stand gehalten wird. Dies ist die Institution, an die sich Österreicherinnen und Österreicher wenden können, wenn sie einen Abzocker- und Betrugsvorfall haben;
- **Internet-Ombudsmann:** Diese Meldestelle bietet Hilfe bei der Streitbeilegung sowie kostenlose Online-Beratung zu allen Aspekten des Einkaufs im Internet. Der Internet-Ombudsmann ist eine staatlich anerkannte Schlichtungsstelle für Streitigkeiten aus Online-Verträgen nach dem Gesetz zur alternativen Streitbeilegung. Er bietet auch

kostenlose Schlichtung und Beratung zu anderen internetbezogenen Themen (Urheberrecht, Datenschutzrecht, Recht am eigenen Bild, Persönlichkeitsrechte usw.) an (Bundesministerium für Digitalisierung und Wirtschaftsstandort1, 2019);

- **Kriminalpolizeiliche Arbeit:** Es wurde eine spezielle Meldestelle eingerichtet, die den Bürgern Informationen zur Verfügung stellt, wenn sie mit einer Cyberkriminalität zu kämpfen haben. Außerdem kann sich eine Person bei Verdacht oder konkreten Hinweisen auf Internetkriminalität an die zuständige Meldestelle des Bundesministeriums des Innern (Bundesministerium für Digitalisierung und Wirtschaftsstandort1, 2019) wenden
- **Saferinternet.at:** Saferinternet.at ist die österreichische Informations- und Koordinationsstelle im Safer Internet Network der EU. Sie unterstützt InternetnutzerInnen mit Tipps und Hilfestellungen bei der kompetenten und sicheren Nutzung von Internet, Mobiltelefonen und Computerspielen. Die Initiative richtet sich speziell an Kinder, Jugendliche, Eltern und Lehrer (Bundesministerium für Digitalisierung und Wirtschaftsstandort1 2019).;
- **Cyber-Security-Hotline:** Im Notfall (z.B. bei einem Cyber-Angriff oder der Verschlüsselung Ihrer Daten durch einen Erpressungstrojaner) kann die Cyber-Security-Hotline unter 0800 888 133 rund um die Uhr kostenlose Hilfe leisten;
- **Kommission für Informationssicherheit:** im Bundeskanzleramt als national und international anerkannte Anlaufstelle Nationale Sicherheitsbehörde für alle Fragen im Bereich der Informationssicherheit und der relevanten Bereiche wie Personalsicherheit, physische Sicherheit, Dokumentensicherheit oder Registerführung und Informationssicherheit sowie nationale Akkreditierungsstelle für inländische Institutionen im Zusammenhang mit der Verarbeitung von geheimen Informationen (Bundesministerium für Digitalisierung und Wirtschaftsstandort2 , 2019).

4.3.2. Tschechien

Die Cybersicherheit ist ein globales Phänomen, das eine Herausforderung für jeden Einzelnen darstellt. Obwohl die Cybersicherheit eine der wichtigsten Herausforderungen ist, mit denen Regierungen heute konfrontiert sind, bleiben die Sichtbarkeit und das öffentliche Bewusstsein

begrenzt. Fast jeder hat schon einmal von Cybersicherheit gehört, aber die Dringlichkeit und das Verhalten der Personen spiegelt das hohe Bewusstsein nicht wider. Einige wichtige Maßnahmen, die von der Öffentlichkeit verfolgt werden:

- **Verfügen über ein legales und regelmäßig aktualisiertes Betriebssystem;**
- **Virenschutz- und Firewall-Software verwenden;**
- **Regelmäßige Aktualisierung des Webbrowsers;**
- **Nutzung von Sicherheitserweiterungen des Domainnamensystems,** die eine Ursprungsauthentifizierung der Daten ermöglichen**;**
- **Verwendung eines sicheren Passworts.**

4.3.3. Portugal

Wenn es eine Situation gibt, in der Menschen mit einem Cybersicherheitsvorfall konfrontiert werden, können sie sich an einige Institutionen wenden. Diese Institutionen werden hier erwähnt:

- **Verband "APDPO Portugal - Associação dos Profissionais de Proteção e de Segurança de Dados":** Dies ist ein Berufsverband, der Einzelpersonen und Organisationen vertritt, sich mit dem Schutz und der Sicherheit von Daten, der Regulierung der Privatsphäre und der elektronischen Kommunikation befasst oder die die Position von Datenschutzbeauftragten in Organisationen, die auf portugiesischem Gebiet tätig sind, innehat;
- **Kontakt- Telefonverbindung "internet segura":** Der Verein Associação Portuguesa de Apoio à Vítima ist für die Verwaltung und die Operationalisierung dieser Leitung verantwortlich. Der Hauptzweck dieser Telefon- und Online-Leitung ist es, bei Zweifeln und Problemen im Zusammenhang mit der Online-Sicherheit, Cybermobbing, Mobbing und unwürdiger Exposition von Jugendlichen, Erwachsenen, Lehrern und Kindern zu helfen und darauf zu reagieren. Die volle Unterstützung ist vertraulich und anonym;
- **Kontakt- Telefonverbindung "Linha aberta":** Diese Telefonverbindung ist auf illegale Inhalte (Kinderpornographie, Gewalt und Rassismus) und die strafrechtliche Verfolgung derjenigen ausgerichtet, die diese Art von Inhalten veröffentlichen.

- **Wenden Sie sich bei Bedarf an die Richtlinienbeauftragten**.

Es ist jedoch wichtig zu sagen, dass die Menschen freien Zugang zu einigen Initiativen (z.B. Maßnahmen, Workshops, Kurse, Tutorials...) haben, um Cybersicherheitsvorfälle zu verhindern.

4.3.4. Spanien

Die Früherkennung von Zwischenfällen ist der Grundstein für die Unterstützung von Maßnahmen und Verfahren, um deren Ausweitung und Auswirkungen zu stoppen und die Wiederherstellung zu erleichtern. Um diese schädlichen Aktionen auf systematische Weise zu erkennen, ist es notwendig, Detektionsmittel zu entwickeln und einzusetzen sowie zentrale Instrumente für das Ereignismanagement zu implementieren. Ein Vorfall sollte, sobald er entdeckt wurde, identifiziert und in seiner Art und seinen Auswirkungen bewertet werden. Er sollte ein Reaktionsverfahren auslösen, das es auf automatisierte Weise ermöglicht, die potenziell geschädigten Personen oder Einrichtungen über die Art und die Hauptmerkmale des Vorfalls zu informieren. Es sollte auch detaillierte Informationen bieten, um die entsprechenden Entscheidungen für seine Bewältigung zu treffen und die folgenden geeigneten Anhaltemaßnahmen zu ergreifen:

1. Sicherheitsparameter für die Wiederherstellung der Anlage;
2. Vertrauliche Daten sichern;
3. Verhinderung von Angriffen, auf integrierte Weise durch die Implementierung von Cyber-Maßnahmen;
4. Integration von Schlüsselfunktionalitäten zur risikolosen Interaktion mit diesen Geräten. Diese Funktionalitäten gewährleisten Zugänglichkeit, Integrität, Vertraulichkeit und Zugangskontrolle;
5. Klassifizierung möglicher Risiken und Bedrohungen;
6. Einbeziehung hochzuverlässige Software.

4.4. Identifizierung der Hauptrisiken/-schwierigkeiten, denen Menschen in ihrem Privatleben in Bezug auf die Cybersicherheit täglich ausgesetzt sind

4.4.1. Österreich

Die Hauptrisiken/-schwierigkeiten, denen die Menschen in ihrem Privatleben täglich ausgesetzt sind, sind:

- **Phishing** durch Datendiebstahl**;**
- **Ransomware (Erpressung, Kryptotrojaner):** Sie nimmt den infizierten Computer praktisch als Geisel und verschlüsselt einzelne Daten und Ordner;
- **Trojaner:** sind meist unbemerkt auf dem Computer und arbeiten im Hintergrund, um Spam-Mails oder DDoS-Angriffe gegen bestimmte Websites oder Unternehmen zu versenden;
- **Viren und Würmer:** was ein Virus oder Wurm letztendlich mit dem eigenen Computer macht, kann nicht vorhergesagt oder begrenzt werden. Am Anfang gab es oft "Scherzviren", die Nachrichten einblenden oder den PC herunterfahren. Trotzdem kann ein solcher Täter einfach alle Daten löschen oder verschlüsseln;
- **Online-Belästigung durch** Cyber-Mobbing, Cyber-Stalking;
- **Betrüger beim Online-Shopping** (gefälschte Geschäfte, Markenfälschungen);
- **Abonnementfallen, versteckte Bedingungen und Konditionen;**
- **Kleinanzeigenbetrug:** nichtexistierende Unternehmen, die gefälschte Nachrichten versenden und dann wird Geld gezahlt, ohne die Ware zu erhalten;
- **Privatsphäre und Datenschutzeinstellungen;**
- **Hoax/Kettenbrief**.

4.4.2. Tschechien

Die Trends der Cyber-Kriminalität wurden den zwischen 2011 und 2016 veröffentlichten Jahresberichten entnommen, die jährlich vom Innenministerium, Abteilung Sicherheitspolitik, veröffentlicht werden. Jeder Bericht über die Lage im Bereich der inneren Sicherheit und öffentlichen Ordnung in der Tschechischen Republik (bis 2016) beschreibt u.a. die Informationskriminalität und die Cybersicherheit für das Vorjahr, z.B. für den Zeitraum von

2010 bis 2015 mit Ausnahme des Jahres 2010 gibt es in allen Berichten die quantifizierten Daten über die Informationskriminalität.

Die häufigsten Ausprägungen dieses Verbrechens sind identisch:

- **Urheberrechtsverletzungen;**
- **Verbreitung von extremistischer und terroristischer Propaganda;**
- **Verbreitung von verbotener Pornographie;**
- **Betrügerisches Verhalten;**
- **Bedrohungen;**
- **Erpressung;**
- **Panikmache;**
- **Beleidigungen;**
- **Angriffe auf Informationssysteme und Daten;**
- **Stalking;**
- **Urheberrechtsverletzungen;**
- **Bedrohungen;**
- **Erpressung und Betrug;**
- **Unbefugte Datenmanipulation;**
- **Betrug** (Fälle von Betrug in der Informationstechnologie und insbesondere im Internet).

Die Gesamtzahl der Cyber-Vorfälle nimmt seit 2011 zu (siehe Tabelle unten). Im Jahr 2015 betrug die Zahl der Cyber-Vorfälle 5.023.

Abbildung 22 - Anzahl der Cyber-Vorfälle (Merkmale der Zeitreihen)

year	number of incidents	absolute growth	relative growth	growth coefficient
2011	1502	-	-	-
2012	2195	693	0.461385	1.461385
2013	3108	913	0.415945	1.415945
2014	4348	1240	0.39897	1.39897
2015	5023	675	0.155244	1.155244

Quelle: Sociálno-Ekonomická revue (2017)

4.4.3. Portugal

Heutzutage sind die Hauptrisiken, denen die Menschen in ihrem Privatleben tagtäglich in Bezug auf die Cybersicherheit ausgesetzt sind Folgende:

- **Virus und Computerwürmer;**
- **Malware-Infektionen durch E-Mail;**
- **Bösartige Software;**
- **Phishing;**
- **Trojaner;**
- **Wurm;**
- **Virus;**
- **Spam;**
- **Betrügerische Links**;
- Personen, die **persönliche Informationen** wie Personalausweisnummer, Zahlungsdaten, Kredit-/Debitkarten- oder Bankkontonummer **einfach online zur Verfügung stellen**;
- Die **missbräuchliche Verwendung von persönlichen Informationen**;
- Der **Zugang von Kindern zu unangemessenen digitalen Inhalten**;
- die **fehlende Beschränkung auf Cookies** aufgrund mangelnder Kenntnisse.

4.4.4. Spanien

Das mangelnde Wissen über die digitale Informationsumgebung stellt eine Schwachstelle in der spanischen öffentlichen Meinung dar. Hier ist eine Liste mit einigen der Schlüsselprobleme, mit denen die Menschen täglich konfrontiert sind:

- **Ransomware.** Die Methoden einer Infektion mit Ransomware:
  - **Remote-Desktop:** neue Möglichkeit, Computer mit Lösegeldern zu infizieren. Es ermöglicht den Fernzugriff auf das System, das später infiziert wird;
  - **Mobile Geräte:** Das Ausmaß der mobilen Lösegeldforderung hat sich im letzten Jahr mehr als verdreifacht;
  - **E-Mail:** Es ist das beliebteste Mittel zur Verbreitung von Ransomware, da es keine geeignete Methode gibt, um den Schutz zu gewährleisten;
  - **Exploits:** Wird verwendet, um Systeme zu infizieren. Ein Beispiel dafür wurde in schlecht geschützten Datenbanken gesehen, wie z.B. bei den Mongo-DB-Angriffen**;**
  - **Fernseher:** Es gab Fälle von Lösegeldforderungen im Zusammenhang mit der Infizierung herkömmlicher Fernsehgeräte, was auf die neu entdeckte Raffinesse dieser Angriffe zurückzuführen ist;
  - **Medjack:** Entführung von medizinischen Geräten, die aus der Integration von traditionellen IKT- und Gesundheitstechnologien resultieren.
- **Distributed-Denial-of-Service (DDoS)- Angriffe.** Die häufigeren Arten von Angriffen dabei sind:
  - **IdD (IOT)-Geräte:** Die Anzahl der anfälligen IdD (IOT)-Geräte hat zum Anstieg des Umfangs von DDoS-Angriffen beigetragen;
  - **DDoS als Dienstleistung**: In der Entwicklung, aufgrund der Reduzierung der Kosten für die zu ihrer Durchführung erforderlichen Tools;
  - **Erpressung:** Erpressungsaktionen unter Androhung von DDoS-Angriffen oder Unterbrechung von Online-Diensten;
- **Hacktivismus.** Diese Angriffe können sogar noch schädlicher sein als traditionelle Bedrohungen, da Hacktivisten oft versuchen, eine Erklärung abzugeben, so dass ihre Bestrebungen in der Regel dem Ruf einer Organisation in der Öffentlichkeit sehr schaden;
- **Botnetze.** Das Eindringen in solche Systeme wird in den kommenden Jahren immer häufiger vorkommen, wobei Lösegeld und Hacktivismus als zentrale Problembereiche gelten. Es besteht auch eine erhebliche Bedrohung der Privatsphäre, da intelligente

Geräte in der Regel eine beträchtliche Menge an sensiblen Informationen enthalten, auf die Cyberkriminelle zugreifen könnten;

- **Manipulation oder Täuschung von Schlüsselpersonen** zur Weitergabe wichtiger Daten oder Finanzinformationen, z.B. durch Phishing-Techniken;
- **Insider-Bedrohungen (Zugang zu vertraulichen Informationen).** Es besteht eine große Wahrscheinlichkeit, dass Cybersicherheitsprobleme intern auftreten. Die meisten externen Bedrohungen sind leicht zu erkennen und zu identifizieren. Davon waren mehr als zwei Drittel der Personen mit böswilligen Absichten, während die übrigen Vorfälle auf "unbeabsichtigte Akteure" zurückzuführen sind. Letzteres bezieht sich auf unschuldige Personen, die Angreifern versehentlich Zugang zu Informationen gewährten oder die Sicherheitsmaßnahmen nicht befolgten;
- **Mobile Malware;**
- **Gefälschte Anzeigen und Feedback.** Die Verbraucher werden häufig mit Online-Werbung bombardiert, und die Verbreitung von gefälschten Anzeigen und Phishing-Angriffen hat das Vertrauen in netzbasiertes Marketingmaterial beeinträchtigt;
- **Cloud-basierte Dienste und Computer;**
- **Informationsfluss zwischen verschiedenen Geräten.** Die meisten Mitarbeiter bringen heutzutage ihre eigenen Geräte mit zur Arbeit, z.B. Smartphones, Tablets und Laptops. Wenn diese Geräte jedoch sowohl als Arbeits- als auch als Privatgeräte verwendet werden, könnte dies die vertraulichen Informationen oder Daten Ihres Unternehmens gefährden;
- **Verwaltung von Mitarbeiterausweisen.** Die Gewährleistung, dass nur die richtigen Mitarbeiter und Auftragnehmer Zugang zu vertraulichen oder abgeschotteten Geschäftsinformationen haben, kann den Unterschied zwischen einer starken Sicherheitsumgebung und der Gefahr von Insider-Cyber-Bedrohungen ausmachen.

4.5. Was wird in Ihrem Land angewandt, um die Internetsicherheit der Bürger in ihrem Privatleben zu verbessern?

4.5.1. Österreich

In Österreich gibt es einige Initiativen zur Verbesserung der Internetsicherheit der Bürger in ihrem Privatleben. Einige von diesen sind:

- **Broschüren** mit grundlegenden Sicherheitstipps für die korrekte Nutzung des Internets und der Computer für die persönliche IT-Sicherheit. Diese Tipps befassen sich mit folgenden Themen: Schutz des PCs; E-Mails und Chat; Software; Filesharing-Netzwerke; Online-Shopping; Bezahlung; Online-Banking im Web; private Informationen, Fotos und Passwörter; Angebote als Waren- oder Finanzagenten; und, Apps und Abo-Fallen. Diese Broschüren werden vom Österreichischen Bundeskriminalamt erstellt;
- **Nachrichten.**

4.5.2. Tschechien

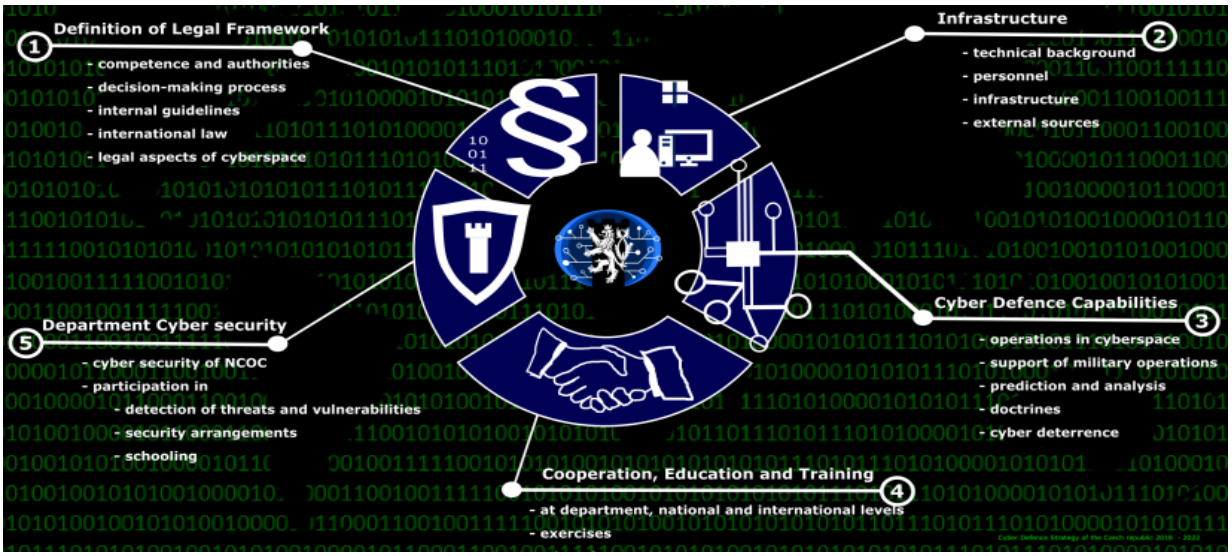
Um die Sicherheit zu verbessern, wird die Cyber-Sicherheitsstrategie der Tschechischen Republik umgesetzt. Die Cybersicherheitsstrategie für die Tschechische Republik umfasst die Jahre 2015 bis 2020.

Die Nationale Cybersicherheitsstrategie der Tschechischen Republik ist ein Dokument, das die Kernwerte, Interessen, Einstellungen, Ambitionen und Instrumente von Tschechien zur Gewährleistung der Sicherheit erklärt und die Grundsätze formuliert, auf denen die Sicherheitspolitik von Tschechien beruht. In dieser Strategie werden lebenswichtige, strategische und andere wichtige Interessen von Tschechien, das Sicherheitsumfeld sowie das Sicherheitssystem von Tschechien beschrieben. Die Sicherheitsstrategie ist das Basisdokument der Sicherheitspolitik von Tschechien. In dem Text wird auf der allgemeinen Ebene auch die Cybersicherheit betont. Diese Strategie baut dann Teilstrategien und Konzepte auf.

Die Grundprinzipien der Cybersicherheitsstrategie: Verknüpfung und Stärkung der Zusammenarbeit aller Bereiche der Gesellschaft; individuelle Verantwortung; Zusammenarbeit

der Abteilungen; internationale Zusammenarbeit; Angemessenheit der getroffenen Maßnahmen; Einsatz zuverlässiger und vertrauenswürdiger Informationstechnologie; und die Sensibilisierung für die Cybersicherheit.

Abbildung 23 – Cybersicherheitsstrategie von Tschechien (2018-2022)



Quelle: National Cyber Operations Center (n.d.)

Es gibt auch noch andere gute Initiativen zu erwähnen, wie zum Beispiel:

- **Projekt "Safer Internet":** Ziel ist es, das Bewusstsein für die Sicherheit im Internet zu erhöhen, illegale, unerwünschte und schädliche Inhalte zu bekämpfen und das Bewusstsein der Endnutzer, Eltern und Lehrer zu schärfen. Der Kampf gegen illegale Inhalte konzentriert sich auf neue Arten der Kommunikation wie soziale Netzwerke. Zu den Hauptzielgruppen des Projekts gehören Kinder und Jugendliche, Eltern, Pädagogen, Spezialisten usw. Weitere Informationen auf dieser Website: https://www.saferinternet.cz;
- **Projekt E-Bezpečí:** Ziel ist es, das Bewusstsein für Prävention, Bildung, Forschung, Intervention und risikoreiches Internetverhalten und damit verbundene Phänomene zu erhöhen. Das Projekt konzentriert sich auch auf den positiven Einsatz von IT in der Bildung und im Alltag in Tschechien. Weitere Informationen auf dieser Website: https://www.e-bezpeci.cz/.

4.5.3. Portugal

In Portugal gibt es einige Initiativen, um die Internetsicherheit der Bürger in ihrem Privatleben zu verbessern. Einige dieser Beispiele sind:

- **Das Konsortium "CNCS"** organisiert mehrere Initiativen: Tipps; Empfehlungen; Broschüren; Sensibilisierungssitzungen; Seminare im Zusammenhang mit der Cybersicherheit und der Förderung des Projekts; Sensibilisierungs- und Schulungsprogramm im Zusammenhang mit der Cybersicherheit; nationale Veranstaltung im Bereich der digitalen Sicherheit, die einmal im Jahr stattfindet; allgemeiner Cybersicherheitskurs und viele weitere;
- **Zwei Telefonverbindungen,** die Menschen helfen, wenn sie Zweifel und Probleme im Zusammenhang mit Online-Sicherheit, Cybersicherheit, Mobbing und unwürdiger Exposition von Jugendlichen, Erwachsenen, Lehrern und Kindern haben;
- **Online-Website "SegurançaNet - Navegar em segurança",** die einer Datenbank ähnelt (mit Präsentationen, Audio-, Pdfs und Videos) und sich an Kinder, Schulen, Jugendliche, Väter und Lehrer richtet. Mit der Initiative "Líderes digitais 2018-2019", die darauf abzielt, die Schülerinnen und Schüler zur Teilnahme an verschiedenen Fächer zu motivieren, die zu einem verantwortungsvolleren Umgang mit der Technologie und der digitalen Umgebung führen;
- **Digitaler Sicherheitsstempel (eSafety-Label**), der eine Zertifizierung verleiht, Schulen unterstützt und darauf abzielt, eine sichere Umgebung im Zusammenhang mit digitaler Technologie als Erfahrung des Lehrens und Lernens zu fördern;
- **Website "Ensina RTP":** Dies ist eine Online-Website, die Informationen (Videos und Kurzmeldungen) zu verschiedenen Themen wie Internetsicherheit bietet;
- **Projekt "Net Segura e Viva":** Dieses Projekt hat zum Ziel, ein sehr nützliches Archiv (mit Informationen, die in häufig gestellten Fragen organisiert sind) mit Ratschlägen aus allen Bereichen der Cybersicherheit anzubieten. Google und Deco Protest führten nicht nur eine Online-Plattform, sondern auch mehrere Konferenzen "NETtalks" über Cybersicherheit in mehreren Städten Portugals durch. Diese nationale Initiative lädt auch alle jungen Leute ein, Videos zu produzieren, um damit zu zeigen, wie wichtig die Teilnahme an sozialen Medien mit Sicherheit und Respekt für die Privatsphäre ist. Die

von den Schülerinnen und Schülern produzierten Videos sollen die sichere Internetnutzung auf kreative Weise fördern, insbesondere in sozialen Medien. Die besten Videos wurden auf der Online-Website veröffentlicht;

- **Projekt "Internet Segura":** Im Hinblick auf den "Europäischen Tag des sicheren Internet", der jedes Jahr, normalerweise im Februar, stattfindet, organisieren zwei Unternehmen (Microsoft und Guarda Nacional Republicana) eine Veranstaltung zu diesem Thema im Umfang von einer Woche mit vielen Aktivitäten im ganzen Land;
- **Zentrum "Centro de Segurança Google":** Seit 2018 gibt Google Zugang zum "Centro de Segurança Google", um seine Nutzer vor Bedrohungen wie Spam, bösartiger Software oder Viren zu schützen. Dieses Zentrum bietet nützliche Informationen, um den Portugiesen eine bessere Kontrolle, Sicherheit und Privatsphäre bei der Online-Navigation zu ermöglichen. Mit dieser Initiative möchte Google Informationen zu vielen Themen, speziell für Familien geben;
- **APDPO Portugal - Associação dos Profissionais de Proteção e de Segurança de Dados":** Dies ist ein Berufsverband, der Einzelpersonen und Organisationen vertritt, die sich mit dem Schutz und der Sicherheit von Daten, dem Schutz der Privatsphäre und der Regulierung der elektronischen Kommunikation befassen oder die die Position von Datenschutzbeauftragten in Organisationen innehaben, die auf portugiesischem Gebiet tätig sind;
- **Projekt "Miúdos seguros na NET":** Dieses Projekt half Familien, Schulen und Gemeinden, die Online-Sicherheit für Kinder und Jugendliche zu fördern. Die wichtigsten verfügbaren Ressourcen sind Artikel (zwischen 2003 und 2008) und ein Blog.

Neben diesen Initiativen fördern einige Unternehmen die Verbreitung von Informationen im Zusammenhang mit der Internetsicherheit in ihren eigenen Websites oder Blogs. In Portugal gibt es auch mehrere Bücher zum Thema Internetsicherheit.

Obwohl es einige Aktivitäten im Zusammenhang mit der Internetsicherheit gibt, spielt die portugiesische Regierung keine aktive Rolle, wenn es um die Förderung von Verbreitungsaktivitäten geht. Wenn jemand ein Problem im Zusammenhang mit dem

Datenschutz oder der Internetsicherheit hat, muss er online nach einer Lösung suchen, sich an einen Anwalt oder eine Person wenden, die über mehr Wissen zu diesen Themen verfügt.

4.5.4. Spanien

Um die Sicherheit zu verbessern, werden verschiedene Verantwortlichkeiten umgesetzt, die im Folgenden beschrieben werden:

- **Projekt Safer Internet Centre Spain (SIC-SPAIN):** Dieses Projekt setzt den Service von Internet Segura for Kids (IS4K) fort und erweitert ihn. Es fördert die sichere und verantwortungsvolle Nutzung des Internets und der neuen Technologien unter Kindern und Jugendlichen. Im Einklang mit der europäischen BIK-Strategie (Better Internet for Kids) ist es Teil des paneuropäischen Netzwerks INSAFE der Internet-Sicherheitszentren. Aufgrund seiner Interoperabilität mit der zentralen Dienstleistungsplattform wird die Finanzierung im Rahmen dieser Aufforderung den verschiedenen europäischen SICs die Aufrechterhaltung und Erweiterung nationaler Plattformen in der gesamten EU durch folgende Dienste ermöglichen:
- **Bewusstsein:** Ein Zentrum zur Sensibilisierung von Kindern, Eltern, Lehrern und anderen Fachleuten, die mit Kindern arbeiten, über die Risiken, denen sie durch Online-Aktivitäten zum Schutz von Minderjährigen ausgesetzt sein können. In Zusammenarbeit mit Dritten werden spezielle Sensibilisierungswerkzeuge und -dienste entwickelt.
- **Informationsdienst:** Online-Hilfsdienste, die junge Menschen, Eltern, Pädagogen und andere Fachleute in diesem Bereich in Fragen des Jugendschutzes im Internet unterstützen.
- **Hotline:** Umfassender Bürgerberichterstattungsdienst, der darauf abzielt, Vorfälle im Zusammenhang mit illegalen Bildern und Videos von sexuellem Kindesmissbrauch im Internet zu empfangen und zu bearbeiten.

Verbesserung der Koordination zwischen den Teilnehmern des Konsortiums sowie mit anderen in diesem Bereich anwesenden und aktiven Akteuren, um eine öffentlich-private Plattform zu schaffen, in der sich verschiedene Einheiten koordinieren, um Sensibilisierungsmaßnahmen

zur Nutzung des Internets bei Minderjährigen mit einer auf nationaler Ebene erweiterten Wirkung durchzuführen.

5. Schlussfolgerung

Die Industrie 4.0 wird von bahnbrechenden Technologien und den Auswirkungen dieser neuen Reindustrialisierung in vielerlei Hinsicht angetrieben, vor allem durch die Bereitstellung von betrieblicher Effizienz und die Herausforderung an etablierte Geschäftsmodelle. Trotz der zahlreichen Vorteile in den Bereichen, die mit Industrie 4.0 verbunden sind, bringt die vierte industrielle Revolution ein neues Betriebsrisiko für angeschlossene, intelligente Hersteller und digitale Versorgungsnetze mit sich.

Die vernetzte Natur von Industrie 4.0 zusammen mit dem Wandel der Digitalisierung bedeutet, dass Cyberangriffe weitaus umfangreichere Auswirkungen haben können als je zuvor. Dies bedeutet, dass es für Organisationen unabdingbar ist, die Auswirkungen dieser Cybersicherheitsrisiken vollständig zu verstehen, bevor sie ihre Cybersicherheitsstrategien anwenden, um sicherer, wachsamer und widerstandsfähiger zu sein und diese vollständig in die Organisationen zu integrieren.

Organisationen müssen sich auf einen Rahmen konzentrieren und verpflichten, der einen integrierten Ansatz für die Cybersicherheit bietet und Fähigkeiten zur Erkennung von Bedrohungen entwickelt, um angemessen und proaktiv zu reagieren. Der Aufbau von Kapazitäten im Bereich der Humanressourcen für Industrie 4.0 muss eine mehrgleisige Strategie intern in den Abteilungen beinhalten.

Um die tatsächlichen Vorteile der vierten industriellen Revolution zu erreichen, müssen die Regierung und auch die Menschen Maßnahmen ergreifen, um sich an die sich entwickelnden Risiken anzupassen.

Die nationalen Regierungen und die öffentlichen Institutionen sollten daher Programme zur Qualifizierung der Arbeitskräfte entwickeln und dafür sorgen, dass der Inhalt dieser Programme in geeigneter Weise modifiziert wird, um in Zukunft alle Kernthemen einzubeziehen. Darüber hinaus sollte die öffentliche Politik den Unternehmen angemessene Anreize für Investitionen in diesem Bereich bieten.

Wenn es um die Menschen geht, besteht auch ein großer Bedarf, die Maßnahmen zur inneren Sicherheit für alle zu verbessern. Daher ist die Erleichterung der Bildung, Ausbildung und Entwicklung von Fähigkeiten ebenso grundlegend. Auch die Notwendigkeit, belastbar zu sein

und eine aufmerksame Haltung zu haben, bringt für die Menschen die Notwendigkeit mit sich, sich besser zu informieren, denn eine sichere Welt ist eine von allen geteilte Verantwortung.
Als nächstes haben wir eine Liste der wichtigsten Barrieren/Schwierigkeiten, mit denen Unternehmen und Bürger konfrontiert sind, sowie einige Empfehlungen zur Verbesserung der Cybersicherheit.

5.1. Vergleichende Analyse zwischen allen Ländern

Industrie 4.0 fördert weltweit verschiedene Veränderungen in Unternehmen und der Gesellschaft, und mit dieser neuen industriellen Revolution hat die Zahl der Angriffe erheblich zugenommen. Infolgedessen sehen sich alle Länder täglich einigen Herausforderungen und Cyber-Angriffen gegenüber, die immer komplexer werden und immer häufiger auftreten.
Seit den letzten Jahren sind alle Länder an der Organisation zahlreicher Initiativen beteiligt, die darauf abzielen, die Antwort auf die wichtigsten Herausforderungen dieser neuen industriellen Revolution und der Cybersicherheit zu verbessern. Die häufigsten Initiativen zu diesem Thema, die in jedem Land vorhanden sind, sind: strategische Länderpläne; möglicher Zugang zu einer gewissen finanziellen Unterstützung; Zugang zu Informationen über einige Plattformen; die Existenz einer öffentlichen Behörde, die in jedem Land beim Datenschutz und der Cybersicherheit hilft (wie CERTs); Cybersicherheitsprojekte (öffentliche und private); und die Existenz nationaler Informationen (z.B. Richtlinien, Orientierungen,...). Trotz aller Initiativen, die es gibt, stehen alle Länder noch immer vor zahlreichen Herausforderungen, und sie müssen mehr investieren und sich Tag für Tag kontinuierlich anpassen.
Darüber hinaus sind einige der häufigsten Herausforderungen, mit denen die analysierten Länder konfrontiert sind: der Mangel an Kompetenzen und Neuqualifizierung der Humanressourcen; fehlende Fähigkeiten zur Erkennung und Bewältigung von Sicherheitsmängeln; fehlende Unterstützung durch öffentliche Behörden/Organisationen; Zusammenarbeit zwischen allen relevanten Stellen auf nationaler Ebene; die Existenz veralteter rechtlicher Grundlagen.
Die häufigsten Cyber-Bedrohungen sind: Malware, Phishing, Malware, Spam, Lösegeld-Angriffe, Datenverletzungen und Trojaner. Die häufigsten Risiken und Schwierigkeiten sind:

Angriffe werden immer komplexer, die Abhängigkeit der Unternehmen von Hardware und Software wächst, die zunehmende Menge an Daten, die geschützt und gesichert werden müssen, sowie fehlende Entwicklungen/Schulungen.
Daher ist die Cybersicherheit heute und mehr denn je eine oberste Priorität für alle, und jedes Land sollte einige Maßnahmen und Aktionen zu diesem Thema einbeziehen.
In den nächsten beiden Abschnitten sehen wir die Hauptschwierigkeiten/Hindernisse und einige Vorschläge/Maßnahmen/Empfehlungen/bewährte Praktiken zur Verbesserung der Cybersicherheit.

5.2. Arbeit/Unternehmen

Die Hauptschwierigkeiten/Hindernisse in den an diesem Bericht beteiligten Ländern in Bezug auf Arbeitnehmer und Cybersicherheit sind:

- Die Angriffe werden immer komplexer und häufiger, und die Hauptmotivation für Angriffe ist die Monetarisierung;
- Die Sicherheit in der Cloud wird zu einem kritischen Thema und es wird erwartet, dass Unternehmen zunehmend von Cloud-Anbietern abhängig werden;
- Die neuen Regeln zum Schutz personenbezogener Daten werden erhebliche Anforderungen an die Unternehmen stellen;
- Die Bedeutung von organisatorischen Maßnahmen (z.B. Risikomanagement) wird in Zukunft gegenüber rein technischen Maßnahmen zunehmen;
- Die Abhängigkeit der Unternehmen von Hard- und Softwareprodukten stellt eine zunehmende Bedrohung dar;
- Es gibt nicht genügend Anreize für Sicherheitsinvestitionen in Unternehmen;
- Mangelndes Sicherheitsbewusstsein und fehlende Standards;
- In Ländern, die das Verständnis und die Anwendung von Sicherheitsmaßnahmen erschweren, gibt es noch immer fehlende oder veraltete rechtliche Grundlagen;
- Mangelndes Sicherheitsbewusstsein bei den meisten Menschen;
- Mangel an ausgebildetem/qualifiziertem Cybersicherheitspersonal und digitalen Kompetenzen;

- Fehlende Schulungsaktivitäten zur Verbesserung der Kenntnisse und ein viel sichereres Verhalten der Menschen;
- Mangelndes Bewusstsein der Mitarbeiter für die kybernetischen Bedrohungen und die IT-Sicherheitsregeln;
- Mangel an klaren und prägnanten technischen Leitfäden zur Cyber- und Internetsicherheit;
- Eskalierende Gehaltsanforderungen an qualifiziertes Cybersicherheitspersonal können die Situation verkomplizieren;
- Viele separate Sicherheitswerkzeuge erhöhen letztlich die operative Komplexität und verringern die Transparenz der allgemeinen Sicherheitslage;
- Organisationen verfügen oft nicht über ein formelles Cybersicherheits-Reaktionsteam oder sogar über eine namentlich benannte Person, die für den Umgang mit einem solchen Vorfall verantwortlich ist;
- Es gibt einen Mangel an Zusammenarbeit zwischen Datenschutz- und Cybersicherheitsteams;
- Viele Unternehmen verfügen über keinen konsistenten Cybersicherheitsreaktionsplan;
- Es fehlt an Zeit und qualifizierten Ressourcen, die für die Umsetzung des Cybersicherheitsplans erforderlich sind;
- Es fehlt ein angemessenes Budget, um die Sicherheitskapazitäten zu erhöhen;
- Veraltete IT-Sicherheitshardware und -software;
- Mangelndes Engagement des Managements und ein unzureichendes Budget;
- Mangelnde Beteiligung aller Mitarbeiter an der Cybersicherheitsstrategie (falls es eine solche gibt);
- Das Inventar der Vermögenswerte mit Auswirkungen auf die Cybersicherheit ist nicht allen Beschäftigten des Unternehmens bekannt;
- Die Kultur der Cybersicherheit muss verinnerlicht werden, Sicherheitsprogramme und -maßnahmen wie Prozesse, Umwelt oder das Management der Prävention von Arbeitsrisiken;
- Nur wenige Initiativen konzentrieren sich auf die industrielle Cybersicherheit;
- Es gibt keine ausreichend getesteten Cybersicherheitslösungen;

- Mangelnde Zusammenarbeit zwischen Unternehmens- und Regierungsinitiativen;
- Ineffiziente Kommunikation zwischen den verschiedenen Teams aufgrund ihrer unterschiedlichen Kenntnisse und Fähigkeiten in Bezug auf den Einsatz von Software und Hardware;
- Es gibt Aktivitäten, die die Systeme und in der Folge die Sicherheit der industriellen Prozesse und Anlagen gefährden können;
- Mangelndes Bewusstsein für die Auswirkungen und die Notwendigkeit neuer Technologien, die zur Gewährleistung der Interoperabilität von Steuerungssystemen eingesetzt werden;
- Die allgemeine Auffassung, dass die Bedrohung ungewiss und ziemlich unwahrscheinlich ist;
- Die Spionage durch moderne digitale Mittel bedroht die nationale Wettbewerbsfähigkeit und Produktivität;
- Unterschiedliche Cybersicherheitsbedürfnisse in den verschiedenen Tätigkeitsbereichen;
- Fehlende finanzielle Unterstützung für die Entwicklung der Cybersicherheit;
- Mangel oder absoluter Mangel an spezifischen Standards für die Cybersicherheit;
- Missverständnis des Themas aufgrund eines Mangels an zielgerichteten Schulungsprogrammen und öffentlichem Kommunikationsmaterial;
- Falsche Implementierung von Sicherheitslösungen und -technologien wie Firewalls, Lösungen IDS/IPS, Antivirus usw.;
- Keine Beziehung oder Vereinbarung zwischen Behörden, Unternehmen und Anbietern in Bezug auf Cybersicherheit;
- Geringe Koordination zwischen den verschiedenen EU-Mitgliedsstaaten.

Um die **Cybersicherheit in Unternehmen zu verbessern, haben wir einige Vorschläge/Maßnahmen/Empfehlungen/gute Praktiken vorgeschlagen**:

- Schulung und Sensibilisierung aller Mitarbeiter im Tagesgeschäft;
- Passwörter sollten immer geheim gehalten werden und einer vordefinierten Richtlinie entsprechen. Außerdem sollte das Passwort regelmäßig geändert werden;

- mehrere Authentifizierungsmethoden verwenden (z.B. Benutzername/Passwort, Antwort auf Sicherheitsfrage, Digitales Zertifikat, Chipkarte, Fingerabdruck, Gesichtserkennung);
- In den Einstellungen eines Wireless-LAN-Routers ist es notwendig, den Verschlüsselungsstandard WPA oder WPA-2 einzustellen. Verfügt das Gerät nicht über eine dieser Einstellungen, muss zumindest der unsichere Standard WEP verwendet werden;
- Implementieren Sie weitere Sicherheitslösungen und Technologien wie Firewalls, Lösungen IDS/IPS, Antivirus usw;
- Antivirenprogramme und Firewalls müssen durch regelmäßige Updates gewartet werden. Dies gilt auch für alle anderen Programme, die auf einem Computer installiert wurden, damit bekannte Sicherheitslücken geschlossen werden können;
- Externe Datenträger (USB-Sticks, externe Festplatten, DVDs etc.) dürfen nicht verwendet werden;
- Implementierung eines geeigneten Ausbildungsprogramms für Studenten und Hochschulabsolventen, das Themen der Cybersicherheit beinhaltet, um auch die Widerstandsfähigkeit der bestehenden Industrieanlagen zu verbessern;
- Entwicklung von Verfahren und Richtlinien zur Verwaltung der Cybersicherheit in komplexen, miteinander verbundenen Umgebungen;
- Erstellung von technischen Leitfäden zur Verbesserung der Kenntnisse der Arbeitnehmer;
- Entwicklung von Methoden und Systemen zur Erkennung von Fehlfunktionen in internationalen Netzwerken;
- Entwicklung von Lösungen für den sicheren Informationsaustausch, um die Reaktion auf Vorfälle der Cybersicherheit im Umfeld von Industrieanlagen zu koordinieren;
- Entwicklung von Techniken zur Erkennung, Verfolgung und Untersuchung von Vorfällen und zur Zusammenarbeit mit Verteidigungsorganisationen;
- Entwicklung von Strategien zur Verbesserung der Informationssysteme im Zusammenhang mit der Cybersicherheit; Entwicklung von Techniken zur Erkennung, Verfolgung und Untersuchung von Vorfällen und zur Zusammenarbeit mit

Verteidigungsorganisationen; Entwicklung von Strategien zur Verbesserung der Informationssysteme im Zusammenhang mit der Cybersicherheit;

- Entwicklung von Standards für verschiedene Bereiche der industriellen Cybersicherheitsumgebung, wie z.B.: Ausrüstung, Interoperabilität und Management, Datenerfassung und -analyse, Tests und Schulungen;
- Organisation von Veranstaltungen und Workshops im Zusammenhang mit der Cybersicherheit für alle Beteiligten und Einzelpersonen;
- Zugriff auf Intranet-Ressourcen über ein virtuelles privates Netzwerk;
- Erstellung einer Strategie zur Reaktion auf Vorfälle;
- Implementierung von Maßnahmen zur Erkennung von Bedrohungen und Entwicklung eines Plans zur Reaktion auf Cybersicherheitsvorfälle;
- Bilden Sie ein Cybersicherheitsreaktionsteam für Vorfälle;
- Implementierung eines Cybersicherheitsrisikoplans in Ihrem Unternehmen/Organisation und jährliche Überprüfung dieses Plans;
- Bewusstsein schaffen über Cyber-Bedrohungen in Unternehmen und deren Auswirkungen auf das Endergebnis;
- Jeder sollte für die Cybersicherheit verantwortlich sein. Unternehmen müssen die Cybersicherheit zu einem zentralen Bestandteil der Geschäftsstrategie und -kultur machen. Einbindung in die strategische Entscheidungsfindung und Nutzen aus der laufenden Innovation und deren Übernahme. Zu diesem Thema siehe z.B.: Talentmanagement; Risiko- und Sicherheitskultur; und, Training und Bewusstsein;
- Wenn man die Cybersicherheit in den Mittelpunkt einer Unternehmensstrategie stellt, wird das Vertrauen der Verbraucher, der Regulierungsbehörden, der Medien und anderer Interessengruppen, die mit den Unternehmen/Organisationen in Verbindung stehen, erhalten und sogar noch gestärkt;
- Entwicklung nationaler Strategien, um Unternehmen bei der Bewältigung/Reaktion auf ihre wichtigsten Cybersicherheits-Unfälle zu helfen, wenn möglich für jeden Tätigkeitsbereich;
- neue Formen von Partnerschaften und Engagement von verschiedenen Arten von Stakeholdern fördern;

- Die Programme, die in Computern und technologischen Geräten verwendet werden, sollten immer mit den neuesten Versionen aktualisiert werden;
- Den Zugang zu bösartigen Websites blockieren und die Kontrolle über das Internet einschränken;
- Schützen Sie das Wi-Fi-Netzwerk mit einem starken Passwort und die Verbindung mit Datenverschlüsselung und ändern Sie auch die Standardeinstellung des verwendeten Routers, indem Sie das Passwort im Einstellungsfenster des Routers ändern;
- Schulung aller Mitarbeiter, da die Mehrheit der Mitarbeiter nicht über ausreichende Kenntnisse und Kompetenzen verfügt, um sich ständig sicherer zu verhalten;
- Sicherungen mit sämtlichen für das Unternehmen relevanten Daten;
- die Mitarbeiter in alle Initiativen so einzubinden, dass sie mit ihrer Erfahrung und ihrem Wissen dazu beitragen können;
- Entwicklung von Programmen, Werkzeugen und Techniken sowie Referenzdokumenten, die die Leistung der Cybersicherheitsexperten unterstützen können;
- Organisation von Schulungsinitiativen, kostenlosen Handbüchern und Workshops, die die verschiedenen Bedürfnisse berücksichtigen;
- Durchführung regelmäßiger Risikobewertungen durch Organisationen.

5.3. Privatleben

Die Hauptschwierigkeiten/Barrieren in Ihrem Land in Bezug auf Menschen und Cybersicherheit sind Folgende:

- Mangelndes Sicherheitsbewusstsein und mangelnde Standards;
- Nachlässiges Verhalten bei der Nutzung des Internets;
- Die aktuellen Studienprogramme beinhalten meistens keine Themen zur Cybersicherheit;
- Es gibt zwar gute Initiativen, Tipps und Hinweise, aber es erreicht nicht die allgemeine Bevölkerung;
- Hohe Anzahl von bösartiger Software auf dem Markt;
- Unzureichendes Verständnis des Status von Cyber-Angriffen;

- Es gibt viele ländliche Gebiete, in denen aufgrund der Lage nicht sehr viele Weiterbildungsangebote möglich sind;
- Hilfe bei Schwierigkeiten ist in der Regel nur telefonisch oder online verfügbar (mit Ausnahme des direkten Wegs zur Polizei). Es wird eine direkte Anlaufstelle benötigt, an die man sich bei Problemen wenden kann;
- Vorschriften, Richtlinien und Gesetze sind nicht benutzerfreundlich formuliert;
- Informationen über die unterstützenden Materialien sind manchmal sehr schwer zu finden (im Internet), diese müssen schneller und einfacher zugänglich sein;
- Verwendung eines schwachen Passworts, eines einzigen Passworts für die Anmeldung bei mehreren Konten und keine Änderung des Passworts;
- Mangel an Studienmaterial über Cybersicherheit;
- Die Menschen haben leichtes Vertrauen in E-Mail-Anhänge;
- Menschen teilen viele persönliche Informationen in sozialen Netzwerken;
- Allgemeines Desinteresse junger Menschen an der Internetsicherheit;
- Mangelndes Bewusstsein für die kybernetischen Bedrohungen und IT-Sicherheitsregeln;
- Es gibt nicht viele Cybersicherheitsplattformen zum Austausch und zur gemeinsamen Nutzung von Informationen;
- Mangelnde finanzielle Unterstützung für die Förderung der Internetsicherheit für die Menschen und die Entwicklung der Cybersicherheit;
- Nur wenige Initiativen konzentrieren sich auf die Internetsicherheit im täglichen Leben;
- Mangel an Bildungs- und Schulungsprogrammen und öffentlichen Materialien über Internetsicherheit;
- Geringe digitale Kompetenz der Endnutzer;
- Den öffentlichen Nutzern fehlt ein grundlegendes Bewusstsein für potenzielle Bedrohungen;
- Es wurde keine Kultur der Cybersicherheit geschaffen;
- Es fehlt ein klarer und prägnanter technischer Leitfaden zur Internet- und Cybersicherheit;

- Das Inventar von Vermögenswerten mit Auswirkungen auf die Cybersicherheit ist nicht gut bekannt;
- Mangelndes Bewusstsein für die Auswirkungen und den Bedarf an neuen Technologien, die zur Gewährleistung der Interoperabilität von Sicherheits-/Kontrollsystemen eingesetzt werden;
- Missverständnis der Cybersicherheit und der Internetsicherheit aufgrund eines Mangels an zielgerichteten Schulungsprogrammen und öffentlichem Kommunikationsmaterial;
- Richtlinien und Verfahren sind aus der Sicht der Cybersicherheit nicht geeignet;
- Cybersicherheitsrisiken sind nicht in Werkzeuge und Systeme integriert;
- Es gibt keine ausreichend getesteten Cybersicherheitslösungen;
- Falsche Implementierung von Sicherheitslösungen und -technologien wie Firewalls, Lösungen IDS/IPS, Antivirus usw;
- Geringe Koordination zwischen den verschiedenen EU-Mitgliedsstaaten.

Um die Cybersicherheit der Bürger in ihrem Privatleben zu verbessern, finden Sie hier Vorschläge/Maßnahmen/Empfehlungen/gute Praktiken zur Verbesserung:

- Verwenden Sie eine Vielzahl von Computerschutzmaßnahmen wie Virenschutz, Firewall und Updates;
- Öffnen Sie keine verdächtigen Dateien, seien Sie vorsichtig mit Bank-E-Mails und klicken Sie nicht auf einen Link;
- Die Leute sollten vorsichtiger sein, was die zu installierende Software betrifft (aufgrund von Malware, Viren,...);
- Den Informationen, die beim Online-Shopping gegeben werden, mehr Aufmerksamkeit schenken, z.B. Zertifikate und Siegel, Bewertungen, Verbraucherschutz, "gesundes Misstrauen";
- Verschlüsselte Verbindungen verwenden;
- Passwörter sollten mindestens 8 Zeichen und eine Kombination aus Groß- und Kleinbuchstaben, Sonderzeichen und Zahlen enthalten und nicht wiederverwendet werden;
- Seien Sie vorsichtiger mit Abonnementsystemen;

- Gehen Sie mit gutem Beispiel voran und sprechen Sie mehr über die Nutzung des Systems und vereinbaren Sie Regeln;
- Machen Sie ein Backup aller Ihrer Daten;
- Implementierung von Schulungsprogrammen und Workshops über Cybersicherheit für Schulen (Studenten und Absolventen);
- Die Notwendigkeit der Überarbeitung der bestehenden Lehrpläne im Bildungsbereich in Bezug auf diese Themen;
- Entwicklung einer Bildungsplattform, um das Wissen der Menschen über Internetsicherheit zu verbessern;
- Sensibilisierung für Sicherheitsmaßnahmen und Technologien wie Firewalls und Virenschutz;
- Erstellung allgemeiner Leitfäden zur Verbesserung der Kenntnisse, die von jedem unabhängig seiner Ausbildung und seines Wissens, leicht verständlich sind;
- Implementierung von mehr Sicherheitslösungen und Technologien wie Firewalls, Lösungen IDS/IPS, Antivirus usw;
- Organisation von Veranstaltungen und Workshops im Zusammenhang mit der Cybersicherheit für alle Beteiligten und Einzelpersonen;
- Installation von Original-Softwareversionen und deren Aktualisierung, wann immer Sie können.

6. Quellen

Ardielli, E., Ardiellli, J. (2017). Cyber security in public administration of the Czech Republic. Sociálně-ekonomická revue: VŠB-TUO. Abgerufen von: https://fsev.tnuni.sk/revue/papers/147.pdf.

Bulletin Průmyslu 4.0. (2019). Národní centrum Průmyslu 4.0. Abgerufen von: https://www.ncp40.cz/files/bulletin-prumyslu-2019-04.pdf.

Bundeskanzleramt, Digitales Österreich (2012). IKT-Sicherheit. Nationale IKT Sicherheitsstrategie Österreich. Wien: BM.I Digitalprintcenter.

Bundeskriminalamt (2015): Schutz vor IT-Kriminalität. Abgerufen von: https://www.finkenstein.gv.at/_Resources/Persistent/94fb6a97ff9fafa801abe506dd7eb3cc5f6f6c31/IT-Sicherheit.pdf.

Bundeskriminalamt[1] (2019): IT-Sicherheit. Abgerufen von: https://bundeskriminalamt.at/news.aspx?id=43534F5A38367453614D493D.

Bundeskriminalamt[2] (2019): IT-Sicherheit: 7 Tipps für Unternehmen und öffentliche Einrichtungen. Abgerufen von: https://bundeskriminalamt.at/202/Internet_kennen/files/IT_Sicherheit_7_Tipps_fr_Unternehmen_Juni2015.pdf.

Bundesministerium für Inneres (2019): Schutz vor IT-Kriminalität. Abgerufen von: https://www.bundeskriminalamt.at/202/Internet_kennen/files/TippsSchutzCybercrime_Juni2015.pdf.

Bundesministerium für Digitalisierung und Wirtschaftsstandort[1] (2019). Meldestellen. Abgerufen von: https://www.onlinesicherheit.gv.at/erste_hilfe/meldestellen/249337.html.

Bundesministerium für Digitalisierung und Wirtschaftsstandort2 (2019). Informationssicherheit – Industrial Security. Abgerufen von: https://www.usp.gv.at/Portal.Node/usp/public?gentics.rs=PDF&gentics.pb=notvisibleposition&contentId=10007.44661.

Busch, J./Soukup, A./Dutzler, H./Loinig, M./Gorholt, A. (2015). Industrie 4.0. Österreichs Industrie im Wandel. PwC Österreich GmbH Wirschaftsprüfungsgesellschaft.

CCI (2018). Spanish Industrial Cybersecurity Roadmap 2013 – 2018. Abgerufen von https://www.cci-es.org/ documents/10694/0/Roadmap+CCI+English/998bbf3c-da70-4781-b40f-83d391f0cf85.

Centro Nacional de Cibersegurança Portugal (n.d.). Abgerufen von: https://www.cncs.gov.pt/.

Cyber Sicherheit Steuerungsgruppe (2018). Bericht Cyber Sicherheit 2018. Wien: Cyber Sicherheit Steuerungsgruppe.

Cyber Sicherheit Steuerungsgruppe (2019). Bericht Cyber Sicherheit 2019. Wien: Cyber Sicherheit Steuerungsgruppe.

Delloite (2017). Industry 4.0 and cybersecurity - Managing risk in an age of connected production. Abgerufen von: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwiFubazxb7jAhUVolwKHUbTA7oQFjAAegQIAxAB&url=https%3A%2F%2Fwww2.deloitte.com%2Finsights%2Fus%2Fen%2Ffocus%2Findustry-4-0%2Fcybersecurity-managing-risk-in-age-of-connected-production.html&usg=AOvVaw0mfdMLmiERC-Aec8s71G2s.

Delloite (n.d.) Indústria 4.0. Abgerufen von:

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=2ahUKEwi15be5x77jAhXXAmMBHanIAvsQFjACegQIARAC&url=https%3A%2F%2Fwww2.deloitte.com%2Fcontent%2Fdam%2FDeloitte%2Fpt%2FDocuments%2Ftransportation-infrastructures-services%2Findustria4_0medidas-pt.pdf&usg=AOvVaw1WbNQpRq0JufT1IYQvw5x0.

EY (2018). Is cybersecurity about more than protection? EY Global Information Security 2018-19. Abgerufen von: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwiEhdODx77jAhUZ8uAKHUcxCGIQFjAAegQIBRAB&url=https%3A%2F%2Fwww.ey.com%2Fen_gl%2Fadvisory%2Fglobal-information-security-survey-2018-2019&usg=AOvVaw2H0YlwJ2GWhy7IEPTTLYMS.

EY (n.d.) Cybersecurity for Industry 4.0 - Cybersecurity implications for government, industry and homeland security. Abgerufen von: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjWlevexb7jAhWLQUEAHTANCa4QFjAAegQIBBAC&url=https%3A%2F%2Fwww.ey.com%2FPublication%2FvwLUAssets%2Fey-cybersecurity-for-industry-4-0%2F%24File%2Fey-cybersecurity-for-industry-4-0.pdf&usg=AOvVaw3Na4d6orEYCSgwo3f3q3Ku.

EY (2018). Cybersecurity regained: preparing to face cyber attacks. 20th Global Information Security Survey 2017-18. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwid7Mv66ZPjAhX1QEEAHZQ-AQkQFjAAegQIABAC&url=https%3A%2F%2Fwww.ey.com%2FPublication%2FvwLUAssets%2Fey-cybersecurity-regained-preparing-to-face-cyber-attacks%2F%24FILE%2Fey-cybersecurity-regained-preparing-to-face-cyber-attacks.pdf&usg=AOvVaw0wrAdSeBMKqIg9uxX4YEC9.

Gabinete de Estratégia e Estudos (2018). A Cibersegurança em Portugal. Abgerufen von:

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=2ahUKEwjNnMPwx77jAhUK-hQKHSLWDY0QFjABegQIBRAC&url=https%3A%2F%2Fwww.gee.gov.pt%2F%3Foption%3Dcom_fileman%26view%3Dfile%26routed%3D1%26name%3DTE56%2520-%2520A%2520Ciberseguran%25C3%25A7a%2520em%2520Portugal.pdf%26folder%3Destudos-e-seminarios%2Ftemas-economicos%26container%3Dfileman-files&usg=AOvVaw1CGUQIIQs7DHKQDX0E5Y-s.

Gabinete de Estratégia e Estudos (2019). Ponto de Situação da Cibersegurança em Portugal. Abgerufen von: https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=imgres&cd=&ved=2ahUKEwjt3-ayzr7jAhULnhQKHaMGDGYQ5TV6BAgBEAg&url=https%3A%2F%2Fwww.gee.gov.pt%2F%3Foption%3Dcom_fileman%26view%3Dfile%26routed%3D1%26name%3DPowerPoint%2520GEE%2520-%2520Coimbra%2520(ENIAP)%25202019-01-26%2520GOB.pdf%26folder%3Destudos-e-seminarios%252Fparticipacao-em-conferencias%252F2019-3%26container%3Dfileman-files&psig=AOvVaw25PWkebk5Fiznu9PuAPFzu&ust=1563544257946449.

Federal Chancellery of the Republic of Austria (2013). Austrian Cyber Security Strategy. Wien.

Fernández, L. España y la ciberseguridad: hora de remangarse. Revista SIC,410, 27-37. Abgerufen von https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomia Industrial/410/LUIS%20FERN%C3%81NDEZ%20DELGADO.pdf.

Gmv Innovation Solutions (n.d.) Cibersegurança. Abgerufen von: https://www.gmv.com/pt/Sectores/SegurancaInformacao/.

Iniciativa Průmysl 4.0 (2015). Ministerstvo průmyslu a obchodu. Abgerufen von:

https://www.mpo.cz/assets/dokumenty/53723/64358/658713/priloha001.pdf

Kaspersky Lab. (2019). Span and phishing in 2012. Abgerufen von: https://securelist.com/spam-and-phishing-in-2018/89701/.

Microsoft (n.d.). Trends in Global Cybersecurity. Abgerufen von: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&cad=rja&uact=8&ved=2ahUKEwiy1tfUyb7jAhVlA2MBHagjB6QQFjAFegQIABAC&url=https%3A%2F%2Finfo.microsoft.com%2Frs%2F157-GQE-382%2Fimages%2FEN-US-CNTNT-eBook-Security-Trends-In-Global-Cybersecurity.pdf&usg=AOvVaw04gc_UHooXgmmdPcO-c-Vx.

Microsoft (2018). Microsoft Security Intelligence Report Volume 23. Abgerufen von: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=2ahUKEwiy1tfUyb7jAhVlA2MBHagjB6QQFjACegQIBRAC&url=https%3A%2F%2Finfo.microsoft.com%2Frs%2F157-gqe-382%2Fimages%2Fen-us_cntnt-ebook-sir-volume-23_march2018.pdf&usg=AOvVaw0OJ4NbRtj5pdkCoWxfQjVP.

Ministerio del Interior España (2017). Estudio sobre la Cibercriminalidad en España. Secretaría de Estado de Seguridad. Abgerufen von http://www.interior.gob.es/documents/10180/8859844/Informe+2017+sobre+Cibercriminalidad+en+Espa%C3%B1a.pdf/a9f61ddb-3fcf-4722-b9d8-802a424a1a70.

Modern massive Data Analysis for Industry 4.0 Industry 4.0 at VŠB-TUO (2016). Faculty of Electrical Engineering and Computer Science VŠB-TUO Czech Republic. Abgerufen von: https://www.czelo.cz/files/prezentace-pozvanky/1-Snasel-2016-e-mail.pdf.

Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020 (2015). Národní bezpečnostní úřad. Abgerufen von: https://www.cybersecurity.cz/data/navratil2014.pdf.

Nic.at GmbH (2018). Bericht Internet-Sicherheit Österreich 2017. Wien: nic.at GmbH.

OECD (2017). Digital Economy Outlook 2017. Abgerufen von: https://www.oecd.org/internet/oecd-digital-economy-outlook-2017-9789264276284-en.htm.

PwC (n.d.). Industry 4.0: Global Digital Operations Study 2018. Abgerufen von: https://www.strategyand.pwc.com/industry4-0.

Pwc (2018). Global Digital Operations 2018 Survey. https://www.strategyand.pwc.com/industry4-0#Download.

Safer Internet (2019). Ministerstvo vnitra České republiky. Abgerufen von: https://www.mvcr.cz/clanek/safer-internet.aspx.

Security Strategy of the Czech Republic (2015). Ministry of Foreign Affairs of the Czech Republic. Abgerufen von: http://www.army.cz/images/id_8001_9000/8503/Security_Strategy_2015.pdf.

Simio (n.d.). Industry 4.0. Abgerufen von: www.simio.com/applications/industry-40.

Spanish Government (2017). National Security Strategy. Government Presidency. Abgerufen von https://www.dsn.gob.es/sites/dsn/files/2017_Spanish_National_Security_Strategy_0.pdf

Spanish Government - CCN-CERT (2018). Cyber threats and trends 2018. National Cryptologic Centre. Abgerufen von https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2997-ccn-cert-ia-09-18-cyberthreats- and-tendencies-executive-summary-2018-1/file.html.

Spanish Government - CCN-CERT (2019). Aproximación española a la Ciberseguridad. Centro Criptológico Nacional. Abgerufen von https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/16-decalogo-

ciberseguridad-2018/file.

Spanish Government - CCN-CERT (2019). Ciberamenazas y tendencias 2019. Centro Criptológico Nacional. Abgerufen von https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3767-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-resumen-ejecutivo-2019/file.html.

Spanish Government - INCIBE (2015). Gestión de riesgos, una guía de aproximación para el empresario. Abgerufen von https://www.incibe.es/protege-tu-empresa/blog/gestion-riesgos-seguridad-informacion.

Spanish Government - INCIBE (2016). Market Trends in Cybersecurity. Spanish National Cybersecurity Institute. Abgerufen von https://www.incibe.es/sites/default/files/estudios/cybersecurity_market_trends.pdf.

Spanish Government - INCIBE (2017). Decálogo de ciberseguridad empresas. Una guía de aproximación para el empresario. Abgerufen von https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_decalogo_ciberseguridad_metad.pdf.

Spanish Government - INCIBE (2018). La ciberseguridad es cosa de todos, establece buenas prácticas. Abgerufen von https://www.incibe.es/protege-tu-empresa/blog/ciberseguridad-cosa-todos-establece-buenas-practicas.

Strategie kybernetické obrany ČR (2018). Národní centrum kybernetických operací. Abgerufen von: http://www.acr.army.cz/assets/informacni-servis/zpravodajstvi/strategie-kyberneticke-obrany.pdf.

Sevillano, F. (2019). Principales incidentes de ciberseguridad en España durante 2018. Abgerufen von https://willistowerswatsonupdate.es/ciberseguridad/ciberataques-en-espana-

2018/.

The Czech Republic opened national cyber security center (2019). National Cyber Security Center. Abgerufen von: https://www.govcert.cz/en/info/events/2456-the-czech-republic-opened-national-cyber-security-center/.

Verein Industrie 4.0 (2016). Österreichischer Normungs-Kompass Industrie 4.0. Abgerufen von: https://plattformindustrie40.at/wp-content/uploads/2016/12/WEB_INDUSTRIE_4.0_ES-2.pdf.

WebsiteBuilderExpert (2018). Which EU Country is Most Vulnerable to Cybercrime. Abgerufen von: https://www.websitebuilderexpert.com/blog/eu-cybercrime-risk/.

Wirtschaftskammer Steiermark (2019). Cyber-security-hotline. Abgerufen von: https://www.wko.at/Content.Node/kampagnen/cyber-security-hotline/index.html#unternehmen.

WKO Bundessparte Information und Consulting (2019). IT-Sicherheitshandbuch für KMU. Abgerufen von: https://www.wko.at/site/it-safe/sicherheitshandbuch.html.

World Economic Forum (2019). The Global Risks Report 2019. Abgerufen von: https://www.weforum.org/reports/the-global-risks-report-2019.