Definition wichtiger Themen der Internetsicherheit, Länderunterschiede

BE SAFE ON THE INTERNET

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

Index

1. Einführung

Heutzutage geht fast jede Information online, und fast jede einzelne Handlung eines normalen Menschen hat eine gewisse Auswirkung - Einfluss auf das NET (soziale Medien, E-Mails, Geldüberweisungen, Cookies usw.).

Des Weiteren hat heutzutage fast alles eine direkte Verbindung zum NET, und dank der 4. industriellen Revolution ist dies nur ein Anfang.

Das Hauptziel dieses Berichts ist es, die wichtigsten Schlussfolgerungen zu zwei Themen zusammenzufassen: Cybersicherheit und Websicherheit sowie persönliche Daten- und Internetsicherheit.

Außerdem gibt es, wie wir im vorherigen Bericht gesehen haben, viele Ähnlichkeiten in den an diesem Projekt beteiligten Ländern bezüglich der oben genannten Themen. Daher hängen die bestehenden Länderunterschiede eher mit einigen Öffnungsklauseln zusammen, die den nationalen Gesetzgebern einen gewissen Spielraum bieten.

2. Wesentliche Schlussfolgerungen

In diesem Abschnitt gibt es eine Liste der wichtigsten Schlussfolgerungen, die im Intellektuellen Output 2 - Rechtliche Aspekte der Internetsicherheit gefunden wurden. Die Schlussfolgerungen sind in zwei Themenbereiche unterteilt.

2.1. Cybersicherheit and Websicherheit

2.1.1. Arbeit/Firmen

- 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 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 mangelnde Standards;
- Es gibt immer noch fehlende oder veraltete rechtliche Grundlagen in Ländern, die das Verständnis und die Anwendung von Sicherheitsmaßnahmen erschweren;
- Mangelndes Sicherheitsbewusstsein bei den meisten Menschen;
- Mangel an geschultem/qualifiziertem Cybersicherheitspersonal und digitalen Kompetenzen;
- Fehlende Schulungsaktivitäten zur Verbesserung der Kenntnisse und ein viel sichereres Verhalten der Menschen;
- Mangelndes Bewusstsein der Mitarbeiter für die Cyber-Bedrohungen und IT-Sicherheitsregeln;
- Fehlen eines klaren und präzisen technischem Leitfadens 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 nicht über einen konsistenten Cybersicherheitsreaktionsplan;
- Es fehlt an Zeit und qualifizierten Ressourcen, die für die Umsetzung des Cybersicherheitsplans erforderlich sind;
- Es fehlt ein angemessenes Budget, das zur Erhöhung der Sicherheitskapazitäten erforderlich ist;
- 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 Mitarbeitern des Unternehmens bekannt;
- Die Cybersicherheitskultur, Sicherheitsprogramme und -maßnahmen wie Prozesse, Arbeitsumgebung oder Risikopräventionsmanagement am Arbeitsplatz, muss verinnerlicht werden;
- 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 fokussierten Trainingsprogrammen 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.

2.1.2. Privatleben

- Mangelndes Sicherheitsbewusstsein und mangelnde Standards;
- Nachlässiges Verhalten bei der Nutzung des Internets;
- Die aktuellen Programme für Studenten 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 auch direkt wenden kann;

- Vorschriften, Richtlinien und Gesetze sind nicht benutzerfreundlich formuliert;
- Informationen über die unterstützenden Materialien sind manchmal sehr schwer zu finden (im Internet) und sie müssen schneller und einfacher zugänglich sein;
- Verwendung eines schwachen Passworts, eines einzigen Passworts, um sich in mehrere Konten einzuloggen, und keine Änderung des Passworts;
- Mangel an Studienmaterialien über Cybersicherheit;
- Menschen öffnen E-Mail-Anhänge mit unbekanntem Inhalt;
- Menschen teilen eine Menge persönlicher Informationen in sozialen Netzwerken;
- Allgemeines Desinteresse junger Menschen an der Internetsicherheit;
- Mangelndes Bewusstsein für die Cyber-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 Cybersicherheitskultur geschaffen;
- Es fehlt ein klarer und prägnanter technischer Leitfaden zur Internet- und Cybersicherheit;
- Das Inventar von Vermögenswerten mit Auswirkungen auf die Cybersicherheit ist kaum bekannt;
- Mangelndes Bewusstsein für die Auswirkungen und den Bedarf an neuen Technologien, die zur Gewährleistung der Interoperabilität von Sicherheits-/Kontrollsystemen eingesetzt werden;
- Missverständnis über die Cybersicherheit und die 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 Tools 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.

2.2. Schutz persönlicher Daten und Internetsicherheit

- Die neuen Regeln zum Schutz personenbezogener Daten stellen erhebliche Anforderungen an die Unternehmen;
- Aufgrund veralteter Rechtsgrundlagen in gewissen Ländern fehlt noch immer das Verständnis und die Anwendung der DSGVO und anderer Rechtsvorschriften zum Schutz personenbezogener Daten;
- Es gibt Divergenzen hinsichtlich der Informationen, Maßnahmen und Verfahren, die für eine ordnungsgemäße Umsetzung der DSGVO notwendig sind, weil viele Unternehmen noch immer nicht genau wissen, was sie tun sollen;
- Die Notwendigkeit, Zugang zu einfachen, klaren und benutzerfreundlichen Informationen zu haben;
- Fehlende/geringe Umsetzung von Maßnahmen zur Erhöhung des persönlichen Datenschutzes im Alltag;
- Mangel an Maßnahmen, Tipps und zugänglichen Schulungen zum Schutz persönlicher Daten für jeden, unabhängig von Alter, Wissen oder geografischer Lage;
- Fehlende Ausbildungsaktivitäten seit den Anfangsstadien;
- Entwicklung der digitalen Staatsbürgerschaft der Schüler durch geeignete Technologien, einschließlich der Online-Kommunikationsetikette und der digitalen Rechte und Pflichten;
- Die Europäer fordern einen stärkeren Schutz der Privatsphäre im Internet;
- Viele Unternehmen erkennen immer noch nicht die Notwendigkeit, die Information und Schulung der Arbeitnehmer in Bezug auf DGSVO zu verstärken;
- Die Mehrheit der Unternehmen benötigt eine erste Bewertung in Bezug auf den

Grad der Konformität und die Angemessenheit der aktuellen Richtlinien und Prozesse, um mögliche Änderungen in Bezug auf die DSGVO korrekt zu identifizieren;

- Die aktuellen Herausforderungen im Zusammenhang mit der Modernisierung, Globalisierung, Technologie und Digitalisierung implizieren eine Überarbeitung des bereits kontinuierlich bestehenden DSGVO-Prozesses;
- Die gesamte Gemeinschaft, die am Schutz personenbezogener Daten beteiligt ist, ist so bald wie möglich einzubeziehen;
- Definieren und überprüfen Sie regelmäßig die Kenntnisse, Fähigkeiten, Eigenschaften und anderen Merkmale, für die Menschen in Bezug auf die zu analysierenden Themen ausgebildet werden können und müssen;
- Förderung der Produktion kreativer und pädagogischer Online-Inhalte für alle Menschen, die einfach und für jeden zugänglich sein müssen;
- Die digitalen Technologien verändern sich ständig, und Lehrer/Ausbilder müssen ständig geschult werden, damit sie helfen und geeignete Schulungsaktivitäten durchführen können;
- Weisen Sie Ihrem Team die Verantwortung für den Datenschutz zu;
- Führen Sie eine detaillierte Dokumentation der Daten, die Sie sammeln, wie sie verwendet werden, wo sie gespeichert sind, welcher Mitarbeiter dafür verantwortlich ist usw.;
- Schulen Sie Ihre Mitarbeiter und implementieren Sie technische und organisatorische Sicherheitsmaßnahmen.

2.3. Cybersicherheit in Europa

In den letzten Jahren hat die Europäische Kommission eine Reihe von Maßnahmen als Alternative eingeführt, um ein sichereres Online-Umfeld in der EU zu gewährleisten. Darüber hinaus arbeitet die Europäische Kommission daran, die Fähigkeiten und die Zusammenarbeit im Bereich der Internetsicherheit zu verbessern und die EU als Akteur im Bereich der Internetsicherheit weltweit zu stärken.

Seit 2017 begann die EU, sich stärker für Maßnahmen der Cybersicherheit zu engagieren und das Vertrauen der Bürger und Unternehmen in die digitale Gesellschaft in Europa zu

stärken, aber erst im Juni 2019 (mit der Verordnung (EU) 2019/881 des Europäischen Parlaments) wurde eine Reihe von Maßnahmen umgesetzt, die auf die Entwicklung einer starken Cybersicherheit innerhalb der EU und die Sicherheit des digitalen Umfelds der EU abzielen. Außerdem ist das Cybersicherheitsgesetz ein Teil der allgemeinen Cybersicherheit der EU und legt einige Melde- und Sicherheitsanforderungen für Betreiber von wesentlichen Diensten und Anbieter digitaler Dienste wie Cloud-Provider fest.

Seit Juni 2019 ist außerdem das europäische Gesetz zur Cybersicherheit in Kraft getreten, das das neue Mandat der ENISA, der EU-Agentur für Cybersicherheit, festlegt und den europäischen Zertifizierungsrahmen für Cybersicherheit festlegt.

Selbst wenn es in jedem Mitgliedsstaat einige Gesetze zur Cybersicherheit gibt, gibt es auch einige Öffnungsklauseln, die den nationalen Gesetzgebern einen gewissen Spielraum bei der Umsetzung der Cybersicherheit lassen. Einige der Länder in Europa (Tschechische Republik, Österreich, Portugal und Spanien) haben einige Gesetze/Richtlinien/Codes, die sich mit Fragen der Cybersicherheit in ihren eigenen Ländern befassen. Dennoch müssen die Vorschriften zur Cybersicherheit noch weiterentwickelt werden, da das Europäische Parlament als Mitgesetzgeber fungiert und jeder Mitgliedsstaat in erster Linie für seine eigene Cybersicherheit verantwortlich ist. Daher ist es notwendig, einige Maßnahmen zur Verbesserung der Cybersicherheit durchzuführen, wie z.B.:

- Die Gesetzgebung zur Cybersicherheit ist nach wie vor unvollständig, und es gibt einige Verzögerungen in Bezug auf dieses Thema auf dem gesamten europäischen Territorium. Daher ist es notwendig, den Informationsaustausch und die Koordinierung zwischen den Akteuren der Gesetzgebung zu verbessern. Zusätzlich sollen der private und öffentliche Sektor zusammenarbeiten, um zur Beantwortung von Fragen der Cybersicherheit beizutragen, die sich ergeben können;
- Politiker und Gesetzgeber müssen einfachere und direktere Rechtsvorschriften entwickeln, die für jeden, unabhängig vom Hintergrund der Person, benutzerfreundlich sein müssen;
- Laut einem Bericht des Europäischen Rechnungshofes "Herausforderungen für eine wirksame EU-Politik im Bereich der Internetsicherheit" haben 80 % der Unternehmen in der EU im Jahr 2016 mindestens einen Vorfall im Bereich der Internetsicherheit erlebt; 69 % haben kein oder nur ein grundlegendes Verständnis für ihre Gefährdung durch Bedrohungen im Internet und 60 % haben die

potenziellen finanziellen Verluste nie geschätzt. Aus diesem Grund muss die Cybersicherheit in den Unternehmen höchste Priorität haben und durch einige Audits/Externe Analysen regelmäßig (z.B. jedes Jahr) bewertet werden. Durch diese Prüfungen haben Unternehmen Zugang zu nützlichen Informationen und wissen, worauf sie sich entwickeln/ausrichten müssen. Daher haben sie die Verantwortung, einige Maßnahmen umzusetzen, um eine bessere Leistung im Bereich der Cybersicherheit zu erzielen;

- Die Gesetzgebung allein garantiert keine Widerstandsfähigkeit und um eine Kultur der Cybersicherheit aufzubauen, muss jedes Unternehmen einen proaktiven und auch reaktiven Plan haben, um auf einige Cybersicherheitsvorfälle zu reagieren, die sich ereignen können;
- Ein klarer Überblick über den Schulungsbedarf und die Schwächen jeder Person in diesem Bereich ist ebenfalls obligatorisch. Daher ist die Erhöhung der Fähigkeiten und des Bewusstseins der Menschen in frühen Stadien obligatorisch und muss in jedem Land so bald wie möglich beginnen. Es ist zum Beispiel wichtig, einige Initiativen zu organisieren und damit zu beginnen, sie in Unternehmen, Schulen und zu Hause umzusetzen. Nach diesem Vorschlag müssen Unternehmen beispielsweise über eine zertifizierte/qualifizierte Person im Bereich der Cybersicherheit verfügen, die den Rest der Teams insbesondere im Softwarebereich und bei den häufigsten Cybervorfällen wie Phishing-Angriffen, Malware, Trojanern, Spam, Lösegeld und gestohlenen Daten schulen kann. Dies ist auch wichtig, um eine Kultur der Cybersicherheit zu entwickeln.

Alle oben genannten Vorschläge zielen darauf ab, ein höheres Maß an Cybersicherheit in der EU zu erreichen und auch effektiver auf Cybervorfälle zu reagieren.

3. Inhaltskatalog

Die wichtigsten Themen zu den beiden im Intellektuellen Output 2 analysierten Themen werden im Folgenden beschrieben.

- **Cloud Security:** Auch bekannt als Cloud-Computing-Security besteht aus einer Reihe von Richtlinien, Kontrollen, Verfahren und Technologien, die zusammenwirken, um Cloud-basierte Systeme, Daten und Infrastruktur zu schützen. Diese Sicherheitsmaßnahmen sind so konfiguriert, dass sie Daten schützen, die Einhaltung gesetzlicher Vorschriften unterstützen und die Privatsphäre der Kunden schützen sowie Authentifizierungsregeln für einzelne Benutzer und Geräte festlegen.
- **Cyberkriminalität:** Jede kriminelle Aktivität, die einen Computer, ein Netzwerkgerät oder ein Netzwerk betrifft. Während die meiste Cyberkriminalität durchgeführt wird, um Gewinn für die Cyberkriminellen zu erzielen, wird Cyberkriminalität auch gegen Computer oder Geräte direkt durchgeführt, um sie zu beschädigen oder zu deaktivieren, während andere Computer oder Netzwerke zur Verbreitung von Malware, illegalen Informationen, Bildern oder anderen Materialien verwenden. Cyberkriminalität kann viele verschiedene Arten von gewinnorientierten kriminellen Aktivitäten umfassen, darunter Lösegeldangriffe, E-Mail, Internetbetrug und Identitätsbetrug sowie Versuche, finanzielle Konto-, Kreditkarten- oder andere Zahlungskartendaten zu stehlen.;
- **Cybersecurity:** Die Praxis des 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;
- **Cyberdiebstahl:** Diebstahl von finanziellen und/oder persönlichen Informationen durch die Verwendung von Computern für deren betrügerische oder andere illegale Nutzung;
- **Datenschutzverletzungen:** Eine absichtliche oder unabsichtliche Freigabe von sicheren oder privaten/vertraulichen Informationen an eine nicht vertrauenswürdige Umgebung. Datenverletzungen können persönliche Gesundheitsinformationen, persönlich identifizierbare Informationen, Geschäftsgeheimnisse und/oder geistiges

Eigentum betreffen;

- **Datenlecks:** Die unbefugte Übertragung von Daten (elektronisch oder physisch) von einer Organisation an einen externen Bestimmungsort. Bedrohungen durch Datenlecks treten in der Regel über das Internet und per E-Mail auf, können aber auch über mobile Datenspeicher wie USB, Stiftlaufwerke, Laptops usw. auftreten;
- **Datenschutz:** Prozesse des Datenschutzes und beinhaltet die Beziehung zwischen der Sammlung und Verbreitung von Daten und Technologie, der öffentlichen Wahrnehmung und Erwartung der Privatsphäre und den politischen und rechtlichen Grundlagen, die diese Daten umgeben. Ziel ist es, ein Gleichgewicht zwischen den Rechten des Einzelnen auf Privatsphäre herzustellen und gleichzeitig die Nutzung der Daten für geschäftliche Zwecke zu ermöglichen;
- **Informationsschutz:** Ein Zweig der Datensicherheit, der sich mit dem richtigen Umgang mit Daten befasst - Einwilligung, Benachrichtigung und gesetzliche Verpflichtungen. Genauer gesagt geht es um praktische Fragen des Datenschutzes: ob und wie Daten an Dritte weitergegeben werden; wie Daten legal erhoben oder gespeichert werden und um regulatorische Einschränkungen (z.B. DSGVO);
- **Datensicherheit:** Eine Reihe von Standards und Technologien, die Daten vor absichtlicher oder versehentlicher Zerstörung, Änderung oder Offenlegung schützen. Die Datensicherheit kann mit Hilfe einer Reihe von Techniken und Technologien angewendet werden, einschließlich administrativer Kontrollen, physischer Sicherheit, logischer Kontrollen, organisatorischer Standards und anderer Schutztechniken, die auf nicht autorisierte oder böswillige Benutzer oder Prozesse beschränkt sind;
- **Internetsicherheit:** Das Wissen um die Maximierung der persönlichen Sicherheitsrisiken des Benutzers in Bezug auf private Informationen und Eigentum im Zusammenhang mit der Nutzung des Internets und den Selbstschutz vor Computerkriminalität im Allgemeinen;
- **Malware:** Jedes Programm oder 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 Kernfunktionen des Computers und das

Überwachen der Computeraktivitäten der Benutzer ohne deren Zustimmung;

- **Phishing:** Eine Form des Betrugs, bei der sich ein Angreifer in einer E-Mail oder in 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 Anmeldedaten oder Kontoinformationen von Opfern;
- **Sicherheitsverstöße:** Ein Vorfall, der zu einem unbefugten Zugriff auf Daten, Anwendungen, Dienste, Netzwerke und/oder Geräte führt, indem die zugrunde liegenden Sicherheitsmechanismen umgangen werden. Eine Sicherheitsverletzung liegt vor, wenn eine Person oder eine Anwendung unberechtigterweise private, vertrauliche oder nicht autorisierte Informationen eingibt;
- **Spam:** Elektronische Nachrichtensysteme, um unerwünschte oder unerwünschte Nachrichten in großen Mengen zu versenden. Die häufigste Form von Spam ist E-Mail-Spam, aber der Begriff gilt auch für jede elektronisch versandte Nachricht, die unaufgefordert und massenhaft versendet wird;
- **Trojaner:** Art von Malware, die oft als legitime Software getarnt ist. Trojaner können von Cyber-Dieben und Hackern eingesetzt werden, die versuchen, sich Zugang zu den Systemen der Benutzer zu verschaffen;
- **Virus:** Ein Computervirus ist eine Art von bösartigem Code oder Programm, das geschrieben wurde, um die Funktionsweise eines Computers zu verändern, und das sich von einem Computer zum anderen verbreiten soll.