Definice "hot topics" internetové bezpečnosti, rozdíly mezi zeměmi

BE SAFE ON THE INTERNET

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

Osnova

1. Úvod 3
2. Hlavní zjištění 4
2.1. Kybernetická a internetová ochrana 4
2.1.1. Práce/ podniky 4
2.1.2. Soukromý život 6
2.2. Ochrana osobních údajů a internetová bezpečnost 7
2.3. Kybernetická ochrana v Evropě 8
3. Katalog pojmů 11

1. Úvod

V dnešní době jsou téměř všechny informace online a téměř každý čin obyčejného člověka má určitý dopad – otisk na síti (sociální média, e-maily, převody peněz, soubory cookie atd.).

Také má téměř vše přímé spojení se sítí a s příchodem 4. průmyslové revoluce je to jen začátek.

Hlavním cílem této zprávy je shrnout nejdůležitější závěry týkající se dvou témat: kybernetická a internetová bezpečnost a ochrana osobních údajů.

Navíc, jak jste se mohli dočíst v předchozí zprávě, v zemích zapojených do tohoto projektu existuje mnoho podobností týkajících se výše uvedených témat. Rozdíly v jednotlivých zemích proto souvisejí více s některými úvodními doložkami, které ponechávají vnitrostátním zákonodárcům určitou volnost.

2. Hlavní zjištění

V následující části poskytujeme seznam hlavních závěrů, které jsou uvedeny v Intelektuálním výstupu 2 - Právní aspekty bezpečnosti internetu. Závěry jsou rozděleny do dvou témat.

2.1. Kybernetická a internetová ochrana

2.1.1. Práce/ podniky

- Útoky jsou stále složitější a častější a hlavní motivací útoků je monetizace;
- Cloudová bezpečnost se stává kritickým problémem a očekává se, že společnosti budou stále více závislé na poskytovatelích cloudů;
- Význam organizačních opatření (např. řízení rizik) v budoucnu vzroste ve srovnání s ryze technickými opatřeními;
- Závislost podniků na hardwarových a softwarových produktech představuje rostoucí hrozbu;
- Nejsou dostatečné pobídky pro investice do bezpečnosti v podnicích;
- Nedostatek bezpečnostních povědomí a standardů;
- V zemích, které obtížně chápou a uplatňují bezpečnostní opatření, stále chybí nebo zastaraly právní základy;
- Nedostatečné povědomí o bezpečnosti u většiny lidí;
- Nedostatek kvalifikovaného personálu kybernetické bezpečnosti a digitálních schopností;
- Nedostatek vzdělávacích aktivit pro zlepšení znalostí a mnohem bezpečnějšího chování lidí;
- Nedostatečné povědomí zaměstnanců o kybernetických hrozbách a bezpečnostních pravidlech IT;
- Chybějící jasné a stručné technické příručky týkající se kybernetické bezpečnosti a bezpečnosti internetu;
- Zvyšování platových požadavků kvalifikovaného personálu kybernetické bezpečnosti může situaci zkomplikovat;
- Mnoho samostatných bezpečnostních nástrojů v konečném důsledku zvyšuje provozní

složitost a snižuje viditelnost v celkové poloze zabezpečení;

- Podniky často nemají formální tým reakce na incidenty v kybernetické bezpečnosti ani jmenovaný jednotlivec, který je odpovědný za řešení takového incidentu;
- Spolupráce mezi týmy v oblasti ochrany soukromí a kybernetické bezpečnosti není dostatečná;
- Mnoho podniků nemá jednotný plán reakce na kybernetickou bezpečnost;
- Nedostatek času a kvalifikovaných zdrojů nezbytných k realizaci plánu kybernetické bezpečnosti;
- Chybějící řádný rozpočet nezbytný k posílení bezpečnostních schopností;
- Zastaralý hardware a software zabezpečení IT;
- Chybějící závazek vedení spolu s nedostatečným rozpočtem;
- Nedostatečné zapojení všech pracovníků do strategie kybernetické bezpečnosti (pokud existuje);
- Inventarizace aktiv s dopadem na kybernetickou bezpečnost není známa všemi pracovníky ve společnosti;
- Kultura kybernetické bezpečnosti musí být internalizována, bezpečnostní programy a opatření, jako je řízení procesů, životního prostředí nebo prevence pracovních rizik;
- Několik iniciativ zaměřených na průmyslovou kybernetickou bezpečnost;
- Nedostatečné testování žádné řešení kybernetické bezpečnosti;
- Nedostatečná spolupráce mezi podnikovými a vládními iniciativami;
- Neefektivní komunikace mezi různými týmy kvůli jejich rozdílům, pokud jde o jejich znalosti a schopnosti ohledně používání softwaru a hardwaru;
- Existují činnosti, které mohou ohrozit systémy a v důsledku toho i bezpečnost průmyslových procesů a zařízení;
- Nedostatečné povědomí o účincích a potřebě nových technologií používaných k zajištění interoperability řídicích systémů;
- Obecné vnímání, že hrozba je nejistá a zcela nepravděpodobná;
- Špionáž moderními digitálními prostředky ohrožuje národní konkurenceschopnost a produktivitu;
- Různé potřeby kybernetické bezpečnosti v různých odvětvích činnosti;
- Nedostatečná finanční podpora rozvoje kybernetické bezpečnosti;
- Nedostatek specifických norem pro kybernetickou bezpečnost;

- Nedorozumění tématu z důvodu nedostatku cílených vzdělávacích programů a materiálů pro veřejnou komunikaci;
- Špatná implementace bezpečnostních řešení a technologií, jako jsou brány firewall, řešení IDS / IPS, antivirus atd.;
- Slabý vztah nebo dohoda mezi úřady, podniky a poskytovateli v souvislosti s kybernetickou bezpečností;
- Malá koordinace mezi různými státními členy EU.

2.1.2. Soukromý život

- Nedostatek povědomí a standardů o bezpečnosti;
- Nedbalé chování při používání internetu;
- Současné vysokoškolské programy většinou neobsahují témata kybernetické bezpečnosti;
- I když existují dobré iniciativy, tipy a rady, ale nedosahuje obecné populace;
- Vysoký počet škodlivého softwaru na trhu;
- Nedostatečné porozumění stavu kybernetického útoku;
- Existuje mnoho venkovských oblastí, ve kterých není z důvodu umístění možné příliš mnoho dalších vzdělávacích nabídek;
- Pomoc s obtížemi je obvykle k dispozici pouze telefonicky nebo online (s výjimkou přímého kontaktu s policií). Je zapotřebí přímé kontaktní místo, na které se lidé mohou v případě problémů také obrátit přímo;
- Předpisy, zásady a zákony nejsou formulovány uživatelsky přívětivým způsobem;
- Informace o podpůrných materiálech je někdy velmi obtížné najít (na internetu) a vyžadují rychlejší a snadnější přístup;
- Slabá hesla, jedno heslo pro přihlášení k více účtům a neměnící se heslo;
- Nedostatek studijních materiálů o kybernetické bezpečnosti;
- Lidé věří e-mailovým přílohám;
- Lidé sdílejí mnoho sociálních informací na sociálních sítích;
- Obecný nezájem mladých lidí o bezpečnost internetu;
- Nedostatečné povědomí o kybernetických hrozbách a bezpečnostních pravidlech IT;
- Není mnoho platforem kybernetické bezpečnosti pro výměnu a sdílení informací;
- Nedostatek finanční podpory na podporu internetového zabezpečení pro lidi a rozvoj

kybernetické bezpečnosti;

- Několik iniciativ zaměřených na bezpečnost internetu v každodenním životě;
- Nedostatek vzdělávacích a školicích programů a veřejných materiálů o bezpečnosti internetu;
- Nízká digitální gramotnost koncových uživatelů;
- Uživatelům chybí základní povědomí o potenciálních hrozbách;
- Není vytvořena kultura kybernetické bezpečnosti;
- Chybějící jasné a stručné technické příručky týkající se bezpečnosti internetu a kybernetické bezpečnosti;
- Soupis aktiv s dopadem na kybernetickou bezpečnost není znám;
- Nedostatečné povědomí o účincích a potřebě nových technologií používaných k zajištění interoperability systémů zabezpečení / kontroly;
- Neporozumění kybernetické bezpečnosti a bezpečnosti internetu kvůli nedostatku cílených vzdělávacích programů a materiálů veřejné komunikace;
- Zásady a postupy nejsou z hlediska kybernetické bezpečnosti vhodné;
- Rizika kybernetické bezpečnosti nejsou integrována do nástrojů a systémů;
- Nejsou dostatečně testována žádná řešení kybernetické bezpečnosti;
- Špatná implementace bezpečnostních řešení a technologií, jako jsou brány firewall, řešení IDS / IPS, antivirus atd.;
- Slabá koordinace mezi různými státními členy EU.

2.2. Ochrana osobních údajů a internetová bezpečnost

- Nová pravidla týkající se ochrany osobních údajů budou klást na společnosti značné požadavky;
- Stále existují chybějící, zastaralé právní základy a jednoduché informace v zemích, které obtížně chápou a uplatňují GDPR a další právní předpisy o ochraně osobních údajů;
- Existence rozdílů týkajících se informací, opatření a postupů nezbytných pro řádné provádění GDPR, protože mnoho společností stále neví, co přesně dělat;
- Potřeba mít přístup k jasným informacím a uživatelsky přívětivým informacím;
- Nedostatek / nízká implementace opatření ke zvýšení ochrany osobních údajů denně;
- Nedostatek opatření, tipů a dostupného školení v oblasti ochrany osobních údajů pro všechny bez ohledu na jejich věk, znalosti nebo zeměpisnou polohu;

- Nedostatek vzdělávacích aktivit od raných fází;
- Rozvoj digitálního občanství studenta pomocí vhodné technologie, včetně etikety online komunikace a digitálních práv a povinností;
- Evropané požadují silnější ochranu soukromí online;
- Mnoho společností stále uznává potřebu posílit informování a školení pracovníků o GDPR;
- Většina společností potřebuje první posouzení týkající se úrovně shody a přiměřenosti současných politik a procesů pro správnou identifikaci možných změn týkajících se GDPR;
- Skutečné výzvy spojené s modernizací, globalizací, technologií a digitalizací znamenají revizi procesu GDPR, který již existuje nepřetržitě;
- Zapojte co nejdříve celou komunitu zapojenou do ochrany osobních údajů;
- Často definovat a přezkoumávat znalosti, dovednosti, atributy a další charakteristiky, na které lidé mohou a musí být školeni, pokud jde o analyzovaná témata;
- Stimulovat produkci tvůrčího a vzdělávacího online obsahu pro všechny lidi, který musí být jednoduchý a přístupný všem;
- Digitální technologie se neustále mění a učitelé / školitelé musí být neustále školeni, aby mohli pomáhat a poskytovat vhodné školicí činnosti;
- Určete své povinnosti v oblasti ochrany údajů;
- Udržujte podrobnou dokumentaci o údajích, které shromažďujete, jak jsou používána, kde jsou uložena, který zaměstnanec je za ně zodpovědný atd.;
- Vyškolte své zaměstnance a implementujte technická a organizační bezpečnostní opatření.

2.3. Kybernetická ochrana v Evropě

Během několika posledních let zavedla Evropská komise řadu opatření jako alternativu k zajištění bezpečnějšího online prostředí v EU. Evropská komise také pracuje na posílení schopností a spolupráce v oblasti kybernetické bezpečnosti, posílení EU jako hráče na poli kybernetické bezpečnosti na celém světě.

Od roku 2017 se EU začala více zavázat k poskytování opatření v oblasti kybernetické bezpečnosti a k posílení důvěry občanů a podniků v digitální společnost v Evropě, ale teprve v červnu 2019 (s nařízením Evropského parlamentu (EU) 2019/881), které byly provedeny

řadu opatření, jejichž cílem je rozvoj silné kybernetické bezpečnosti v EU a bezpečnost digitálního prostředí EU. Zákon o kybernetické bezpečnosti je rovněž součástí celkové kybernetické bezpečnosti EU a stanoví některé požadavky na oznamování a zabezpečení provozovatelů základních služeb a poskytovatelů digitálních služeb, jako jsou poskytovatelé cloudu.

Od června 2019 navíc vstoupil v platnost evropský zákon o kybernetické bezpečnosti, kterým se stanovil nový mandát agentury ENISA, Agentury EU pro kybernetickou bezpečnost a zřídil se evropský rámec pro certifikaci kybernetické bezpečnosti.

I když existují právní předpisy týkající se kybernetické bezpečnosti, které jsou v platnosti v každém členském státě, existují také některé úvodní doložky, které ponechávají vnitrostátním zákonodárcům určitou volnost ohledně provádění kybernetické bezpečnosti. Některé země v Evropě (Česká republika, Rakousko, Portugalsko a Španělsko) mají některé právní předpisy / směrnice / kódy, které se zabývají otázkami kybernetické bezpečnosti v jejich vlastních zemích. Předpisy o kybernetické bezpečnosti však stále potřebují další rozvoj, protože Evropský parlament funguje jako spoluzákonodárce a každý členský stát nese odpovědnost za svou vlastní kybernetickou bezpečnost. Je proto nezbytné provést některá opatření s cílem zlepšit kybernetickou odolnost, jako například:

Právní předpisy týkající se kybernetické bezpečnosti jsou stále neúplné a na evropském území dochází k určitým zpožděním v této oblasti. V důsledku toho je nezbytné zlepšit výměnu informací a koordinaci mezi aktéry právních předpisů a soukromým a veřejným sektorem, který by měl spolupracovat a přispívat k řešení otázek kybernetické bezpečnosti, které mohou nastat;

- Tvůrci politik a zákonodárci musí vyvinout jednodušší a přímější právní předpisy, které musí být uživatelsky přívětivé pro každého bez ohledu na pozadí dané osoby;
- Podle zprávy Evropského účetního dvora „Výzvy k účinné politice EU v oblasti kybernetické bezpečnosti" zažilo v roce 2016 nejméně jeden incident s kybernetickou bezpečností 80 % podniků v EU; 69 % nemá žádné, nebo pouze základní porozumění jejich vystavení kybernetickým hrozbám a 60 % nikdy odhadlo možné finanční ztráty. Z tohoto důvodu musí být kybernetická bezpečnost ve společnostech nejvyšší prioritou a musí být pravidelně vyhodnocována prostřednictvím některých auditů / externích analýz (například každý rok). Díky těmto auditům mají organizace přístup k užitečným informacím a vědí, na co se musí vyvinout / zaměřit. Z tohoto důvodu mají odpovědnost

za provádění některých akcí s cílem dosáhnout lepší výkonnosti v oblasti kybernetické bezpečnosti;

- Samotná legislativa nezaručuje odolnost a buduje kulturu kybernetické odolnosti, kterou musí každá společnost mít proaktivní a také reaktivní plán, aby reagovala na některé případy kybernetické bezpečnosti, ke kterým může dojít;
- Je také nutné mít jasný přehled o vzdělávacích potřebách a slabostech každé osoby v této oblasti. Proto je zvyšování dovedností a povědomí lidí od raných fází povinné a musí se začít v každé zemi co nejdříve. Například je důležité organizovat některé iniciativy a začít je implementovat ve firmách, školách a doma. Podle tohoto návrhu musí společnosti například mít certifikovanou / kvalifikovanou osobu v oblasti kybernetické bezpečnosti, která může poskytnout školení ostatním týmům, zejména v softwarové oblasti, a nejčastější počítačové incidenty, jako jsou: phishingové útoky; malware; Trojské koně; spam; ukradený ransomware a data. To je také důležité pro rozvoj kultury kybernetické bezpečnosti.

Všechny výše uvedené návrhy mají za cíl dosáhnout vyšší úrovně kybernetické bezpečnosti v EU a také účinněji reagovat na počítačové incidenty.

3. Katalog pojmů

Nejdůležitější témata týkající se dvou témat analyzovaných v Intelektuálním výstupu 2 jsou popsána níže.

- **Zabezpečení cloudu**: známé také jako zabezpečení cloud computingu se skládá ze sady zásad, ovládacích prvků, postupů a technologií, které spolupracují na ochraně cloudových systémů, dat a infrastruktury. Tato bezpečnostní opatření jsou nakonfigurována tak, aby chránila data, podporovala dodržování předpisů a chránila soukromí zákazníka a nastavovala pravidla ověřování pro jednotlivé uživatele a zařízení;
- **Kybernetická kriminalita:** každá trestná činnost, která zahrnuje počítač, síťové zařízení nebo síť. Zatímco většina počítačových trestných činů je prováděna za účelem dosažení zisku pro počítačové zločince, některé počítačové trestné činy jsou prováděny přímo proti počítačům nebo zařízením přímo za účelem jejich poškození nebo deaktivace, zatímco jiné používají počítače nebo sítě k šíření malwaru, nelegálních informací, obrázků nebo jiných materiálů. Počítačová trestná činnost může zahrnovat mnoho různých typů trestné činnosti zaměřené na zisk, včetně útoků na ransomware, e-mailů, internetových podvodů a podvodů s totožností, jakož i pokusů o krádež finančních údajů, kreditních karet nebo jiných informací o platebních kartách;
- **Kybernetická bezpečnost:** praxe ochrany systémů, sítí a programů před digitálním útokem. Cílem těchto kybernetických útoků je obvyklý přístup, změna nebo zničení citlivých informací, vydávání peněz od uživatelů nebo přiblížení běžných obchodních procesů;
- **Kybernetická krádež:** krádež finančních a / nebo osobních údajů pomocí počítače pro účely podvodného nebo soukromého použití;
- **Narušení dat:** úmyslné nebo neúmyslné zveřejnění bezpečných nebo soukromých / důvěrných informací do nedůvěryhodného prostředí. Úniky dat: neoprávněné předávání dat (elektronicky nebo fyzicky) z organizace do vnějšího místa určení. Porušení údajů umožňuje osobní údaje o zdraví, informace umožňující identifikaci osob, obchodní tajemství nebo duševní vlastnictví; K hrozbám úniku dat obvykle dochází prostřednictvím webu a e-mailu, ale může k nim dojít také prostřednictvím mobilních zařízení pro ukládání dat, jako jsou USB, pera, notebooky atd.;
- **Ochrana údajů:** proces ochrany údajů a zahrnuje vztah mezi shromažďováním a

šířením údajů a technologií, vnímáním a očekáváním soukromí ze strany veřejnosti a politickými a právními základy těchto údajů. Jeho cílem je nalézt rovnováhu mezi individuálními právy na soukromí a zároveň umožnit využívání údajů pro obchodní účely;

- **Ochrana osobních údajů:** ochrana osobních údajů je odvětví bezpečnosti údajů, které se týká správného zacházení s údaji – souhlas, oznámení a regulační povinnosti. Konkrétněji se praktická ochrana osobních údajů týká: toho, zda nebo jak jsou data sdílena s třetími stranami; jak jsou údaje zákonně shromažďovány nebo ukládány a regulační omezení (např. GDPR);
- **Zabezpečení dat:** soubor standardů a technologií, které chrání data před úmyslným nebo náhodným zničením, úpravou nebo zveřejněním. Zabezpečení dat lze aplikovat pomocí řady technik a technologií, včetně administrativních kontrol, fyzického zabezpečení, logických kontrol, organizačních standardů a dalších ochranných technik, které se omezují na neautorizované nebo škodlivé uživatele nebo procesy;
- **Internetová bezpečnost:** znalost maximalizace osobních bezpečnostních a bezpečnostních rizik uživatele u soukromých informací a majetku souvisejících s používáním internetu a sebeochranou před počítačovou kriminalitou obecně;
- **Malware:** jakýkoli program nebo soubor, který je škodlivý pro uživatele počítače. Typy malwaru mohou zahrnovat počítačové viry, červy, trojské koně a spyware. Tyto škodlivé programy mohou vykonávat řadu různých funkcí, jako je krádež, šifrování nebo mazání citlivých dat, změna nebo únos základních počítačových funkcí a sledování činnosti uživatelů počítačů bez jejich svolení;
- **Phishing:** je forma podvodu, při níž se útočník maskuje jako renomovaná entita nebo osoba prostřednictvím e-mailu nebo jiných komunikačních kanálů. Útočník používá phishingové e-maily k distribuci škodlivých odkazů nebo příloh, které mohou provádět různé funkce, včetně extrahování přihlašovacích údajů nebo informací o účtu od obětí;
- **Narušení bezpečnosti:** jakákoli událost, která má za následek neautorizovaný přístup k datům, aplikacím, službám, sítím nebo zařízením tím, že obchází základní bezpečnostní mechanismy. K narušení bezpečnosti dochází, když jednotlivec nebo aplikace neoprávněně zadají soukromé, důvěrné nebo neoprávněné informace;
- **Spam:** systémy elektronických zpráv pro hromadné rozesílání nevyžádaných nebo nežádoucích zpráv. Nejběžnější formou nevyžádané pošty je e-mailový spam, ale tento

termín se vztahuje také na všechny zprávy zaslané elektronicky, které jsou nevyžádané a hromadné;

- **Trojský kůň**: typ malwaru, který je často maskován jako legitimní software. Trojský kůň je šířen zloději a hackery, kteří se snaží získat přístup k uživatelským systémům;
- **Virus:** počítačový virus je typ škodlivého kódu nebo programu napsaného za účelem změny způsobu práce počítače a je navržen tak, aby se šířil z jednoho počítače do druhého.