
[ICT] GROUP
ZÁKLADY
CYBERSECURITY
PRO MAJITELE
FIREM
A MANŽERY
OWN IT. SECURE IT. PROTECT IT.


[ICT] GROUP

Obsah

OWN IT.
SECURE IT.
PROTECT IT.

Úvod

Kyberkriminalita a kybernetické útoky jsou každým dnem častější. Více než polovina malých a středních podniků (SMB) uvedla, že se stala obětí kybernetické kriminality. Každý den se objevují nové titulky o únicích dat, hackerských útocích, kybernetických útocích a různých formách trestné činnosti. V průzkumu se více než dvě třetiny zúčastněných podniků staly obětí alespoň jednoho kybernetického útoku, přičemž jedna třetina zažila útok v posledních 12 měsících.

66 % malých podniků se velmi obává kybernetického bezpečnostního rizika.

Kyberkriminalita představuje pro podniky významnou hrozbu. Může vést k narušení provozu, úniku obchodních údajů, údajů o zákaznících, neoprávněnému přístupu a dalším problémům. Průměrné náklady na narušení bezpečnosti dat činí závratných 149 000 USD. Kromě toho se 80 % SMB obává, že se v příštích šesti měsících stanou terčem kybernetické kriminality.

Kybernetické útoky navíc zůstávají problémem ať už mluvíme o cloudu nebo o e-mailech.

Mnoho vládních institucí přešlo na cloud, ale hledají lepší způsoby ochrany svých dat. Součástí toho je i posílení spolupráce mezi zpravodajskými službami a orgány činnými v trestním řízení po celém světě v boji proti trestné činnosti.

Obliba chytrých telefonů a zvýšené používání aplikací představují také významné riziko pro mobilní bezpečnost. Spotřebitelé používají aplikace k zadávání citlivých informací, jako jsou osobní, finanční a bankovní údaje. Tyto aplikace se budou muset vyvíjet s novými technologiemi tak, aby se dokázaly bránit útokům a únikům dat.

Navíc se stále více aplikací přesouvá

Procento organizací, které **NEMAJÍ** nasazená tato kritická kybernetická bezpečnostní řešení

51 % malých podniků tvrdí, že na kybernetickou bezpečnost nevyčleňuje žádný rozpočet.

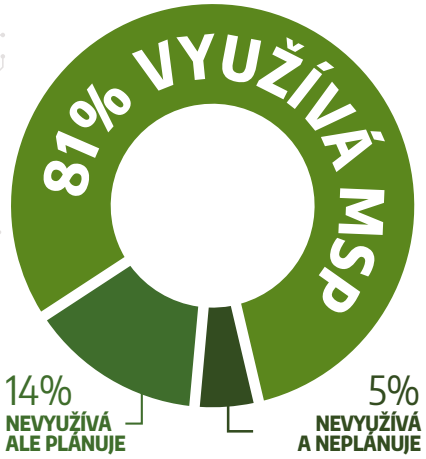
do cloudu a útočníci se stále lépe vyhýbají odhalení pomocí standardních bezpečnostních systémů a protokolů. Šíření ransomwaru a krádeže citlivých dat jsou na vzestupu, protože organizační data se dostávají mimo kontrolu společnosti.

Z jednoduchého malwaru se ransomware stal sofistikovanějším a účinnějším. Kyberzločinci se nyní zaměřují na místní zálohy, jejich kompromitace znemožňuje snahu bezpečnostních pracovníků o obnovení zašifrovaných dat.

Tato hrozba se již neomezuje pouze na místní sítě, ransomwarové útoky zůstávají problémem i v cloudových prostředích.

E-mail zůstává nejoblíbenější metodou kyberzločinců. Více než 91 % útoků je iniciováno e-mailem. Tradiční antivirové programy nedokážou rozpoznat phishingové útoky používané hackery.

Využívání MSP organizacemi



MSP - Managed Service Provider
Poskytovatel spravovaných IT služeb

Škodlivý software může být do systému doručen a spuštěn bez vědomí uživatele, a to i na dlouhou dobu.

Je třeba zvýšit tempo vývoje komplexních řešení kyberkriminality. Ve výše uvedeném průzkumu se 75 % podniků domnívá, že je třeba klást větší důraz na prevenci kyberkriminality.

Mezi skutečností a očekáváním je však velký rozdíl. Většina podniků je nedostatečně kvalifikovaná, pokud jde o aspekty kybernetické kriminality. To vytváří nepříznivou situaci, protože organizace nejsou schopny se před kyberzločinci chránit.

Zde se stává klíčovou role poskytovatelů spravovaných IT služeb (MSP). MSP mohou malé a střední podniky nasměrovat na správnou cestu a pomoci jim chránit se před zvýšeným výskytem kyberkriminality. MSP mohou klienty informovat o potřebě komplexního bezpečnostního řešení a o vývoji prostředí kyberkriminality. MSP by také měli malým a středním podnikům poskytnout kompletní soubor bezpečnostních řešení, aby mohly zůstat chráněny a minimalizovat rizika.

MSP mohou pomoci překlenout mezeru mezi současnou úrovní ochrany a optimální úrovní, kterou si podniky přejí. Podniky si tuto skutečnost uvědomují a spojují se s MSP, aby eliminovaly kybernetické útoky a hrozby a předcházely jim.

Osm z deseti dotazovaných malých a středních podniků spolupracuje s MSP a čtyři z nich chtějí i nadále spolupracovat se svými současnými bezpečnostními partnery. Tři z deseti firem plánují v následujících měsících přejít k jinému MSP. 12 % malých a středních podniků, které nespolupracují s MSP, plánuje během příštích dvanácti měsíců navázat polupráci s MSP.

9 z 10 zaměstnanců tvrdí, že by jejich organizace zvážila přechod k novému MSP, pokud by nabízel řešení, které by splňovalo jejich potřeby.

Na otázku, jaký přínos očekávají od využití MSP, odpovědělo padesát procent malých a středních podniků, že vyšší bezpečnost, a to i v případě, že kybernetickou bezpečnost zajišťují externě.

MSP mohou být ideálním partnerem pro SMB v boji proti kyberkriminalitě, protože 62 % společností nemá potřebné vlastní kompetence.

Spravované IT týmy mohou vyvinout a zavést bezpečnostní opatření a dokonce i rozvrhnout plán obnovy pro případ pravděpodobných útoků. MSP pomáhají organizaci udržet si přehled o trendech v oblasti kybernetické bezpečnosti a umožňují jí s plnou jistotou čelit vyvíjejícím se kybernetickým hrozbám.

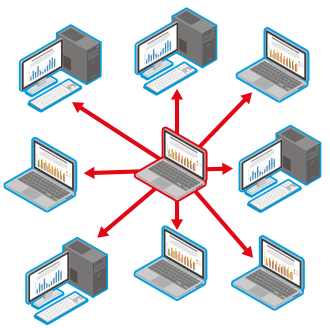
Spolupráce s MSP (nebo MSSP) může pomoci ochránit firmu nebo organizaci před hrozbami nebo útoky a je často nejlepší volbou pro malé a střední firmy, které se tak mohou více věnovat inovacím + růstu a méně času věnovat IT a kybernetické bezpečnosti.

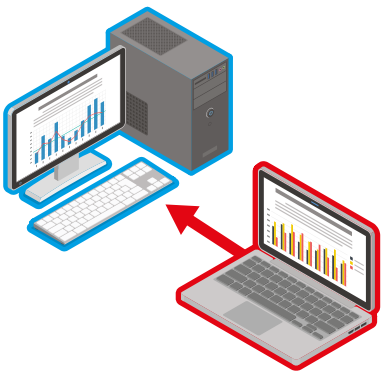
PHISHING & SPEAR PHISHING

Spear phishing neboli cílený phishing spočívá v zasílání e-mailů se škodlivými přílohami, jejichž cílem je krádež osobních údajů. Phishingový útok může také vést oběť na nelegální webové stránky, které ukradnou hesla, údaje o kreditních kartách, obchodní informace a další citlivé údaje. Phishingový útok využívá k dosažení svých cílů technické lsti a sociální inženýrství.

Útočníci využívající phishing si pečlivě vybírají své cíle a vydávají se za důvěryhodný zdroj, o kterém oběti méně pochybují. Útočníci také používají personalizované zprávy, díky nimž e-maily vypadají relevantně a důvěryhodně. V důsledku toho může být pro malé a střední podniky náročné chránit se před útoky typu spear phishing. Phishing je jednou z nejběžnějších forem kybernetických hrozeb.

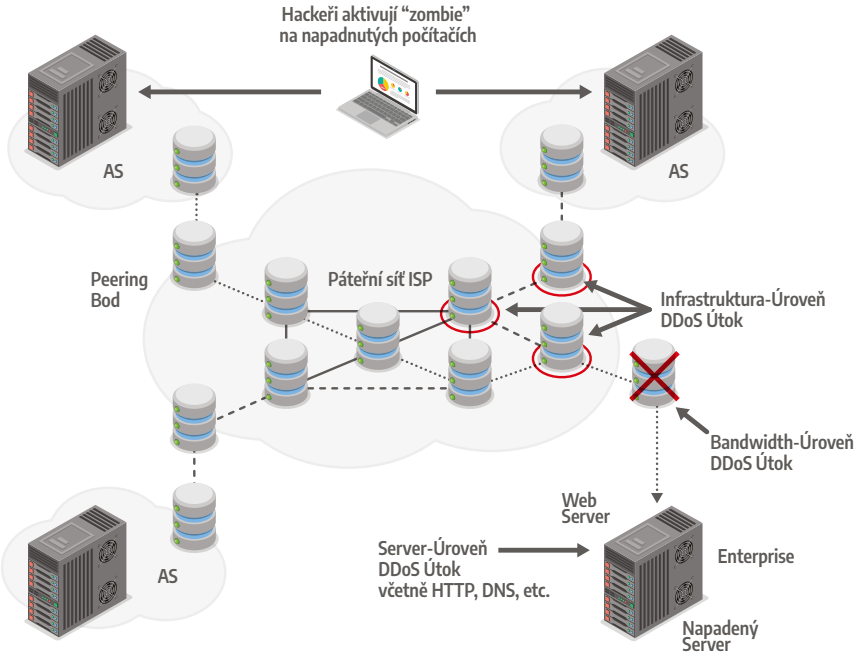
PHISHING	SPEAR [CÍLENÝ] PHISHING
ZPŮSOB	
Spray & Pray (náhoda)	Cílený útok
CÍLENÍ	
Široké & Automatizované	Konkrétní zaměstnanec a/nebo společnost
HACKING ÚROVEŇ	
Ne příliš sofistikovaná	Vyžaduje pokročilé techniky
ÚTOK	
Běžně odhalitelný	Obtížnější odhalení
CO CHTĚJÍ ÚTOČNÍCI ZÍSKAT	
Uživatelská jména, hesla, údaje o kreditních kartách atd.	Důvěrné informace, obchodní tajemství atd.





V ROCE 2020
byl phishing zodpovědný za více než 80 % nahlášených bezpečnostních incidentů.

PRŮMĚRNÉ NÁKLADY NA DDOS ÚTOK $20-40K



DISTRIBUOVANÉ ODEPŘENÍ SLUŽBY (DDOS)

Distribuované odepření služby (DDoS) je útok, který je zaměřen na zdroje serveru, sítě, webové stránky nebo počítače s cílem vyřadit je z provozu nebo narušit jejich služby. Útoky DDoS mají zpravidla hostitelský systém, který napadá další počítače nebo servery připojené k síti.

Útoky DDoS přetěžují systém neustálými požadavky na připojení, oznámeními a provozem. V důsledku toho systém odmítá požadavky na služby legitimních uživatelů. Útoky DDoS nepřinášejí přímý prospěch útočníkovi, protože nekradou žádné informace, pouze „zatěžují" systémy, takže nemohou správně fungovat. Útoky DDoS nicméně mohou být pro podniky škodlivé, protože mohou zastavit provoz a způsobit škody, které často dosahují až statisíců dolarů, například v důsledku ušlých příjmů, ztráty produktivity a poškození dobrého jména.

Mezi lednem 2020 a březnem 2021 se počet **DDoS útoků zvýšil o 55%**

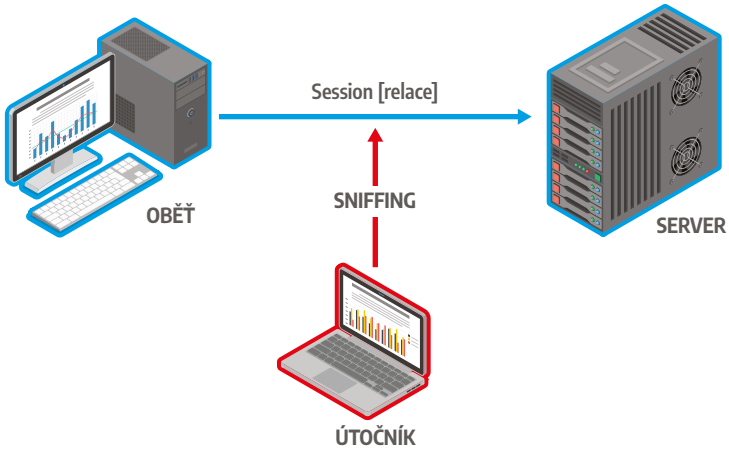
MAN-IN-THE-MIDDLE (MITM) ÚTOK

K útoku MitM dochází, když se hacker vloží mezi komunikaci klienta a serveru. Zde je příklad útoku typu man-in-the-middle:

Session Hijacking

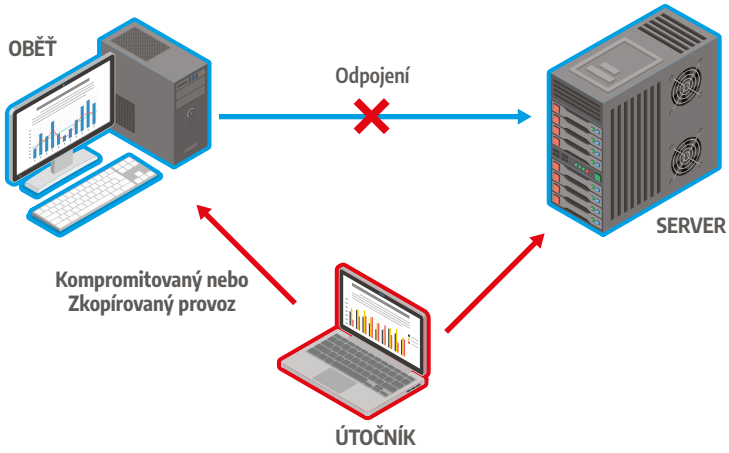
Kyberzločinci používají únos relace, aby získali kontrolu nad relacemi oběti a získali přístup ke zdrojům nebo datům. Nejběžnější metodou je podvržení IP adresy, kdy únosce použije IP adresu důvěryhodného klienta, aby mohl využívat neautorizované služby serveru nebo aplikace.

KROK 1: Zachycení [únos] session [relace]



95 PROCENT WEBOVÝCH SERVERŮ JE **ZRANITELNÝCH** K **MitM** ÚTOKŮM

KROK 2: Přesměrování komunikace přes útočníka



Více než jedna z pěti malých firem nemá vůbec žádný security plán.

HROZBY

Makroviry

Makroviry se zaměřují na inicializační sekvenci aplikace a ohrožují tak programy jako je Microsoft Excel nebo Word.

Trojské koně

Trojské koně jsou nereplikující se viry, které získávají neoprávněný přístup do systému. Trojské koně se často maskují do podoby legitimního softwaru.

Napadení systému nebo spouštěcího záznamu

Tyto viry se připojují ke spustitelným kódům umístěným v zaváděcích částech disku. Viry infikující zaváděcí záznamy se mohou připojit k hlavním zaváděcím záznamům pevného disku a dokonce i k zaváděcím sektorům USB flash disků. Tyto viry se inicializují, když někdo spustí systém pomocí napadeného disku nebo jednotky.

Polymorfní viry

Polymorfní viry se replikují donekonečna, aby sabotovaly systémy. Pokaždé používají dynamické šifrovací klíče, aby se vyhnuly odhalení.

Skryté [Stealth] viry

Stealth viry se skrývají pod rouškou systémových funkcí.

Souborové viry

Souborové viry nacházejí cestu do systému prostřednictvím spustitelných kódů jako jsou přípony .exe. Virus se stane aktivním, když přistoupíte k souboru .exe nebo spustitelnému kódu.

Logické bomby

Logické bomby jsou části škodlivých kódů, které se inicializují při splnění předem definovaných podmínek. Útočníci mohou logické bomby naprogramovat tak, aby sloužily k různým účelům.

Červi

Červi nepotřebují hostitelský soubor, aby se mohli šířit v síti nebo systému. Jsou to samostatné formy virů.

Droppery

Droppery pomáhají virům najít cestu do sítí a systémů. Většinou váš antivirový program droppery nezjistí, protože neobsahují škodlivý kód - pouze k němu vedou!

Ransomware

Ransomware může mít podobu jakéhokoli viru, který drží data oběti jako rukojmí za výkupné. Útoky ransomwaru často zašifrují data nebo soubory a požadují peníze výměnou za dešifrovací klíče.

66 dnů

Početní dní nutný na odhalení kyber útoku

MALWARE ÚTOK

Malware neboli škodlivý software je určen k ohrožení systému za určitým účelem. Uživatel si může nevědomky stáhnout malware, který infikuje systém a šíří se dál. Malware může být navržen tak, aby se choval mnoha způsoby, stejně jako software. Mezi oblíbené typy malwaru patří např:

1. Makroviry
2. Trojské koně
3. Napadení systému nebo spouštěcího záznamu
4. Polymorfní viry
5. Stealth viry
6. Souborové infikátory
7. Logické bomby
8. Červi
9. Droppery
10. Ransomware

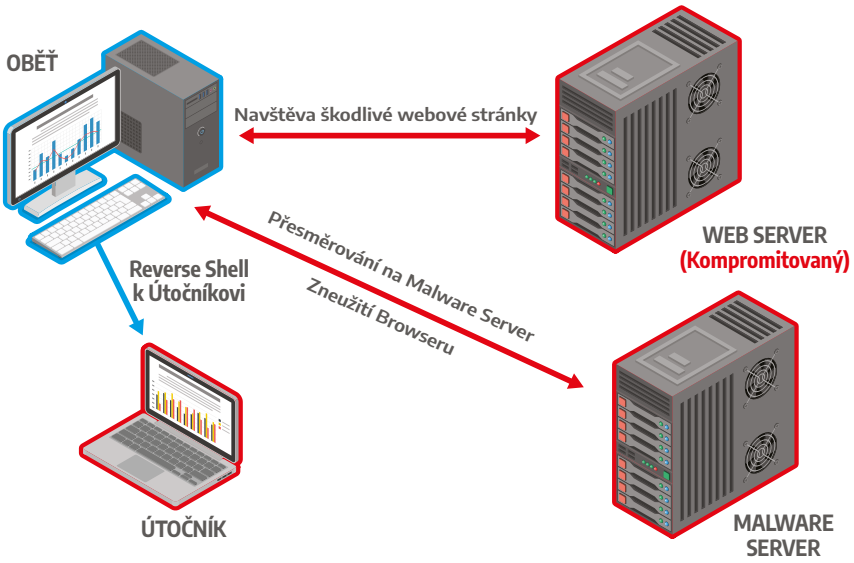
600%

Nárůst Kyber kriminality díky COVID-19 pandemii

DRIVE-BY ÚTOKY

Útoky typu drive-by nebo drive-by downloads představují infikování počítače malwarem, když uživatel navštíví škodlivé webové stránky. K útokům typu drive-by dochází bez vědomí uživatele. Ke stažení a spuštění malwaru v počítači může stačit pouhá návštěva infikované webové stránky.

Útoky také probíhají na pozadí a nejsou pro uživatele viditelné. V důsledku toho nelze podniknout žádné konkrétní kroky k identifikaci nesprávných kódů. Pouze proaktivní přístup může podnikům pomoci chránit se před útoky typu drive-by.



92 PROCENT
malwaru je doručeno e-mailem.

POLOVINA
všech kyber-útoků je konkrétně cílena na malé firmy

V 2018 HACKEŘI UKRADLI **160 000 000** OSOBNÍCH ÚDAJŮ

73 PROCENT
hesel je duplicitních.

ÚTOKY NA HESLA

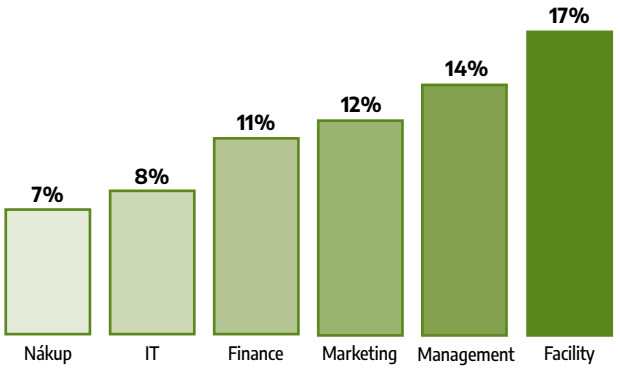
Útoky na hesla umožňují kyberzločincům získat neoprávněný přístup k uživatelským účtům a sítím. Někdo ve vaší kanceláři může heslo jednoduše uhodnout nebo se rozhlédnout po vašem stole a ukrást ho. Proto se vždy doporučuje hesla nezapisovat. Útočníci mohou také špehovat vaši síť, používat dešifrovací nástroje a hrubou silou prolamovat vaše hesla.

Před útoky na hesla vás může zachránit řada bezpečnostních opatření. Můžete nastavit systém tak, aby po několika špatných heslech zablokoval účty. Používání dvoufázového ověřování je také vynikajícím způsobem, jak ochránit své účty před zvědavýma očima.

98 PROCENT
kyber-útoků spoléhá na Social engineering.

KDO NALETÍ NA PHISHING?

Průměrná míra selhání, podle oddělení

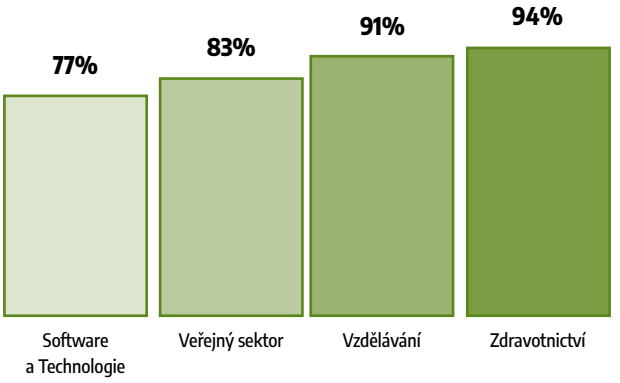


POJIŠTĚNÍ KYBERNETICKÝCH RIZIK

Pojištění obvykle kryje 59 % výkupného, pokud je zaplaceno

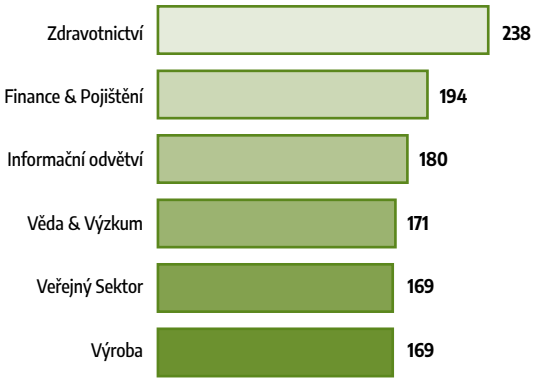
MÍRA OPAKOVANÉHO POUŽÍVÁNÍ HESEL

Hlášené opakované použití hesel zaměstnanců v jednotlivých odvětvích



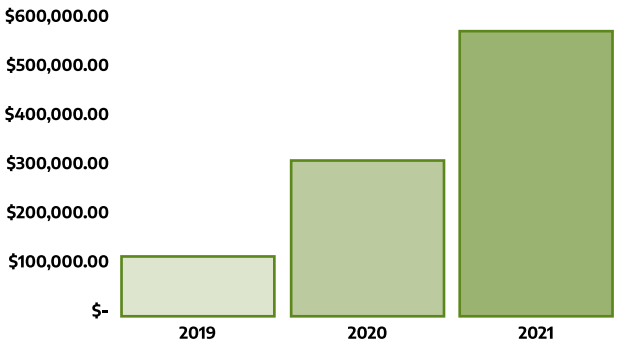
KDO BYL NAPADEN V ROCE 2021?

6 nejčastěji napadaných sektorů v roce 2021



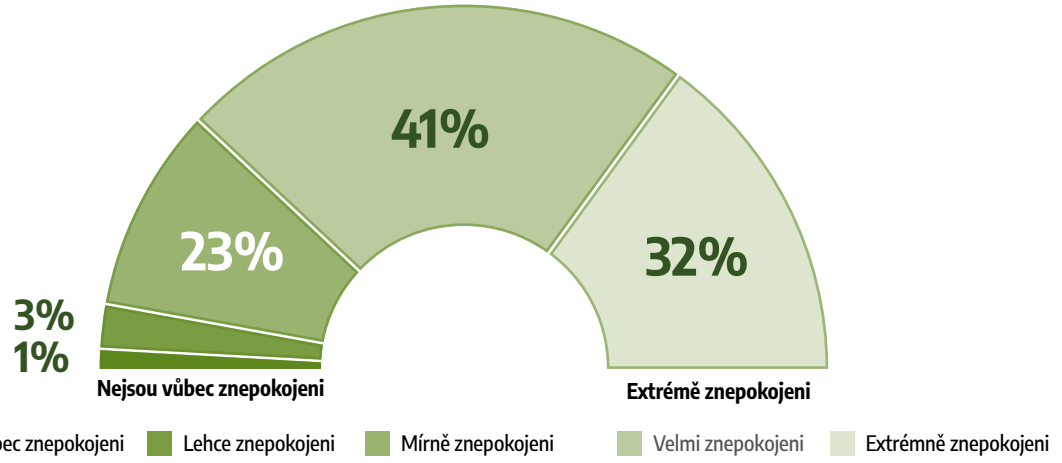
PRŮMĚRNÁ VÝŠE VÝKUPNÉHO

82% nárůst typické skutečně vyplacené částky v roce 2021



ZABEZPEČENÍ CLOUDU

73 % firem je velmi až extrémně znepokojeno



5 klíčových prvků efektivního programu kybernetické bezpečnosti:

1. Útok učí obranu
Poznatky ze skutečných útoků, které ohrozily váš systém, mohou vést k účinné a praktické obraně. Pro dosažení nejlepších výsledků by vaše obrana měla být postavena pouze na kontrolních prvcích, které se osvědčily při prevenci skutečných útoků.

2. Stanovení priorit
Firmy by se měly zaměřit pouze na kontroly, které mohou co nejefektivněji snížit riziko a ochránit organizaci před nebezpečnými kybernetickými hrozbami. Kontroly by také měly být dobře proveditelné, aby je bylo možné implementovat do IT prostředí.

Dílčí kontroly, které je třeba zavést, můžete určit na stránkách CIS Implementation Groups.

3. Měření a metriky
Měli byste mít zavedené standardní metriky nebo klíčové ukazatele výkonnosti, aby všechny zúčastněné strany jako jsou IT vedoucí pracovníci, úředníci a auditoři měli stejný pohled na věc. Metriky jsou nezbytné pro sledování účinnosti vašich bezpečnostních opatření a pro jejich zlepšování.

4. Průběžná diagnostika a prevence
Vždy byste měli být proaktivní a sledovat účinnost svých bezpečnostních opatření. Případné problémy je třeba řešit co nejdříve, aby byla zajištěna integrita následujících opatření.

5. Automatizace
Automatizace pomáhá podnikům zajistit soulad s kontrolními mechanismy a získat škálovatelný a spolehlivý způsob boje proti kybernetickým hrozbám. Automatizace také zvyšuje efektivitu a šetří čas i práci.

CIS Controls™ je soubor osvědčených **bezpečnostních postupů,** které pomáhají podnikům minimalizovat rizika a chránit se před **nejčastějšími** kybernetickými útoky a hrozbami.

Tyto postupy byly vyvinuty a jsou udržovány odborníky na IT a bezpečnost v **Center for Internet Security (CIS)** a jsou uznávány podniky a vládami po celém světě.

Seznam Kontrolních Mechanismů (CIS) P20

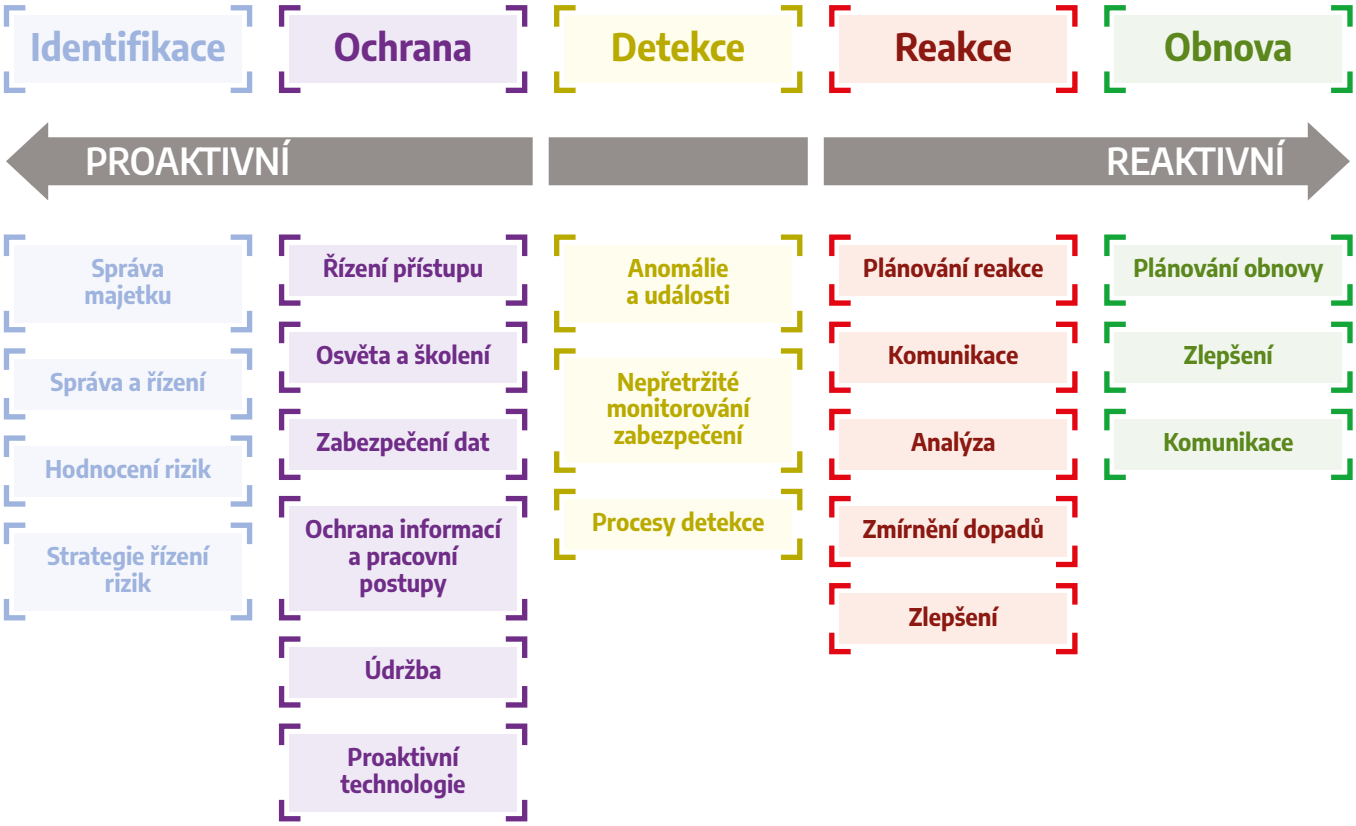
NIST Cybersecurity Framework

NIST Cybersecurity Framework umožňuje firmám a podnikům vyhodnocovat rizika, se kterými se setkávají. Framework se skládá ze tří částí.

Framework Core představuje řadu odkazů, výstupů a činností spojených s aspekty a přístupy ke kybernetické obraně. Úrovně implementace **Frameworku** pomáhají organizacím stanovit jejich přístup ke kybernetické bezpečnosti a objasnit jejich postoj všem zúčastněným stranám. Úrovně také znázorňují stupeň propracovanosti přístupu k řízení bezpečnosti.

Framework Profily obsahují soubor výstupů, které podnik vybral z kategorií a podkategorií na základě svého hodnocení rizik a požadavků. Organizace si mohou na základě Frameworku vytvořit "**aktuální profil**", který obsahuje činnosti a cíle v oblasti kybernetické bezpečnosti, o které podnik usiluje. Poté může organizace sestavit "**Cílový profil**" nebo přejít na tzv. baseline profil, který odpovídá specifickým potřebám organizace v daném odvětví.

Nakonec může organizace vytvořit realizovatelné kroky k dosažení cílového profilu.



CIS Controls™

CIS Controls™ je soubor 18 opatření, která tvoří osvědčené postupy pro řešení závažných útoků na systémy a sítě. Osvědčené postupy vypracovala skupina IT odborníků s dlouholetými zkušenostmi v oblasti kybernetické bezpečnosti. Pocházejí z řady odvětví, včetně státní správy, obrany, zdravotnictví, školství, maloobchodu, výroby a dalších. CIS Controls jsou považovány za sbírku osvědčených bezpečnostních postupů na mezinárodní úrovni.

V průběhu let se na podniky zaměřily různé formy kybernetických útoků. Patří mezi ně úniky dat, krádeže informací o kreditních kartách, krádeže identity a duševního vlastnictví, odepření služby, narušení soukromí a mnoho dalších. Odborníci vyvinuli řadu bezpečnostních protokolů, které mají těmto kybernetickým hrozbám čelit a které se označují jako kybernetická obrana.

IT odvětví využívá k boji proti kybernetickým hrozbám množství zdrojů a nástrojů. K dispozici máme také různé technologie, bezpečnostní kontroly, databáze zranitelností, certifikace, školicí materiály a kontrolní seznamy zabezpečení. Máme přístup ke studiím a zprávám, nástrojům, oznamovacím službám a dalším informacím, které nás chrání před jakoukoli formou kybernetické hrozby. IT průmysl je také závislý na řadě předpisů, security frameworků a bezpečnostních požadavků chránících před kybernetickou kriminalitou.

Přetížení informacemi a technologiemi však často vede ke zmatku. Konkurující si bezpečnostní opatření a možnosti mohou organizaci ochromit v tom, aby podnikla potřebné kroky k boji proti kyberkriminalitě. V současné době se obchodní procesy stávají složitějšími spolu s rozšiřováním mobilních zařízení a rozšiřováním závislostí. Technologický pokrok vedl k šíření dat několika kanály, a to i mimo organizaci. V důsledku toho se bezpečnost v tomto propojeném světě změnila ze samostatného problému na mnohostrannou hrozbu.

Průměrné náklady na útok ransomwaru na podniky činily $133 000.

Tato situace vyvolává potřebu jednat jako komunita a přijít s řešeními a podporou pro různá odvětví, sektory a partnerství. Musíme využít naše znalosti a pokrokové technologie k vytvoření řešení, která řeší klíčové aspekty přístupu organizace k řízení rizik. Takový přístup bude krokem správným směrem a pomůže podnikům učinit správné kroky k řešení bezpečnostních problémů. Nejlepším způsobem, jak toho dosáhnout, je řídit se plánem zásad, které organizacím pomohou rozvíjet jejich kybernetickou obranu a bezpečnostní postupy.

CIS Controls™ byly vyvinuty na základě výše uvedených zásad, aby pomohly organizacím zaujmout komplexní přístup ke kybernetické bezpečnosti. Původně byly vytvořeny jako základní program, který má pomoci omezit nejasnosti a zaměřit se na základní opatření, která umožňují podniku překonat kybernetické hrozby. Kontrolní mechanismy jsou ze své podstaty cenné a poskytují organizacím údaje a znalosti, které jim umožňují zůstat ve střehu, reagovat a předcházet kybernetickým útokům.

CIS Controls™ jsou vedeny celosvětovou komunitou CIS®, která nabízí:

- Sdílený vhled do problematiky kybernetické kriminality, kybernetických útoků a hrozeb s cílem zjistit příčinu problémů a navrhnout vhodná opatření.
- Dokumentace všech požadovaných schválení a distribuce kritických nástrojů.
- Sledování specifik hrozby, včetně jejího růstu, závažnosti a intenzity.
- Zdůraznění významu CIS Controls™ pro zajištění jejich souladu s regulačními rámci.
- Sdílení znalostí, pracovních nástrojů, překladů a dalších informací.
- Řešení běžných hrozeb dříve, než se stanou vážnými, a zavádění plánů jejich řešení v rámci komunity.

CIS Controls se skládají z vysoce funkčního souboru opatření, která mohou organizace implementovat, používat a rozšiřovat. Tyto kontroly jsou také v souladu s většinou platných zákonů a bezpečnostních opatření a jsou podporovány komunitou IT.

Našim klientům pomáháme sladit se s CIS Controls™ a pomoci jim tak zabezpečit jejich podnikání.

Zásady účinné kybernetické obrany

Jak jsme již uvedli, existuje pět zásad spolehlivého programu kybernetické bezpečnosti:

Útok se stává zdrojem informací pro obranu: Vytvářejte účinnější bezpečnostní opatření na základě zkušeností z minulých útoků a hrozeb. Měly by se zvažovat pouze kontroly, které se osvědčily jako účinné.

Stanovení priorit: Stanovte priority kontrolních mechanismů, které byly v reálném světě účinné v boji proti hrozbám. V úvahu by se měla brát také snadnost implementace.

Měření a metriky: Měření a metriky jsou nezbytné pro posouzení účinnosti bezpečnostních opatření. Umožňují také všem zúčastněným stranám v bezpečnostním týmu mluvit stejným jazykem.

Průběžná diagnostika a zmírňování následků: Pravidelně testujte a vyhodnocujte bezpečnostní protokoly, abyste mohli zavést další kroky.

Automatizace: Automatizujte své činnosti v oblasti kybernetické bezpečnosti, abyste zajistili shodu s předpisy a získali spolehlivou a škálovatelnou kybernetickou obranu.

Osvědčené postupy CIS Controls pomáhají podnikům čelit kybernetickým útokům a hrozbám a předcházet jim. Kontroly jsou rozděleny do tří kategorií - základní, fundamentální a organizační kontroly.

IMPLEMENTAČNÍ SKUPINY

CIS chápe, že ne každá firma nebo organizace má prostředky, rozpočet nebo požadavky na řádné zavedení všech doporučených ochranných opatření.

V rámci boje proti kyber zločinu jsou všechna **ochranná opatření** pod každou **kontrolou** rozdělena do **skupin pro implementaci.**

Každá **implementační skupina** navazuje na předchozí, takže **IG2** zahrnuje všechna **ochranná opatření** z **IG1** a **IG3** zahrnuje všechna ochranná opatření z **IG1** i **IG2.**

Dobrým cílem pro organizaci nebo podnik jakékoli velikosti je začít s implementací všeho, co je součástí **implementační skupiny 1 (IG1).**

Po implementaci všech ochranných opatření **IG1** mohou v závislosti na požadavcích a rozpočtu začít implementovat **ochranná opatření** z **implementační skupiny 2 (IG2).**

Nakonec, opět v závislosti na požadavcích a rozpočtu, mohou začít implementovat **ochranná opatření** z **implementační skupiny 3 (IG3).**

Každá z 18 kontrol CIS má řadu **ochranných opatření**, která jsou její součástí. Celkem jich je 153. Těchto 153 **ochranných opatření** je rozděleno do tří (3) skupin:
Implementační skupina 1 (IG1) má 56, **Implementační skupina 2 (IG2)** má 74 & **Implementační skupina 3 (IG3)** má dalších 23 ochranných opatření.

Implementační skupina 1 (IG1) - Základní kybernetická hygiena

Ve většině případů je podnik **IG1** obvykle malý až středně velký a má omezené odborné znalosti v oblasti IT a kybernetické bezpečnosti, které může věnovat ochraně IT majetku a personálu. Obvyklým zájmem těchto podniků je udržet provoz podniku, protože mají omezenou toleranci k výpadkům.

Implementační skupina 2 (IG2)

Firma **IG2** obvykle zaměstnává jednotlivce nebo externí stranu, například poskytovatele spravovaných služeb (Managed Service Provider, MSP), aby jí pomohli spravovat a chránit IT infrastrukturu. Tyto podniky mají obvykle více oddělení s různými rizikovými profily na základě pracovních funkcí a poslání.

Implementační skupina 3 (IG3)

Firma **IG3** obvykle zaměstnává specializované bezpečnostní odborníky, kteří se specializují na různé aspekty kybernetické bezpečnosti. Aktiva a data podniku IG3 obvykle obsahují citlivé informace a často podléhají regulačnímu dohledu a dohledu nad dodržováním předpisů.

01 - Inventarizace a kontrola majetku podniku

Bezpečnostní opatření celkem 5 | IG1 2/5 | IG2 4/5 | IG3 5/5

Aktivně spravovat (inventarizovat, sledovat a korigovat) veškerá podniková aktiva (zařízení koncových uživatelů, včetně přenosných a mobilních, síťová zařízení, nepočítačová zařízení/internet věcí (IoT) a servery) připojená k infrastruktuře fyzicky, virtuálně, vzdáleně a v rámci cloudových prostředí, abyste přesně znali všechna aktiva, která je třeba v podniku sledovat a chránit. To také podpoří identifikaci neautorizovaných a nespravovaných aktiv, která je třeba odstranit nebo korigovat.

Proč je tato kontrola CIS kritická?

Podniky nemohou bránit to, o čem nevědí, že mají. Řízená kontrola všech podnikových aktiv hraje klíčovou roli také při monitorování zabezpečení, reakci na incidenty, zálohování a obnově systému. Podniky by měly vědět, která data jsou pro ně kritická a správná správa aktiv pomůže identifikovat ta podniková aktiva, která tato kritická data uchovávají nebo spravují tak, aby bylo možné použít vhodné bezpečnostní kontroly.

Externí útočníci nepřetržitě skenují internetový adresní prostor cílových podniků, ať už v prostorách podniku nebo v cloudu, a identifikují možná nechráněná zařízení připojená k podnikové síti. Útočníci mohou využívat nově nainstalovaná, ale dosud bezpečně nenakonfigurovaná a nezáplatovaná aktiva. Interně neidentifikovaná zařízení mohou mít také nedostatečné konfigurace zabezpečení, které je mohou učinit zranitelnými vůči malwaru založenému na webu nebo e-mailu, a jakmile se útočníci dostanou dovnitř, mohou využít nedostatečnou konfiguraci zabezpečení k průchodu sítí.

Věděli jste, že?

Téměř 66 % IT manažerů má neúplnou evidenci svého IT majetku. Znalost toho, jaké IT vybavení máte a kde se nachází, je klíčovou funkcí. Můžeme vám pomoci s úvodním auditem majetku a průběžnou správou seznamu majetku.

BEZPEČNOSTNÍ OPATŘENÍ

1.1 Vytvoření a udržování podrobného podnikového inventáře majetku
Zařízení | Identifikace | ● ● ●

1.2 Řízení neautorizovaných prostředků [zařízení]
Zařízení | Reakce | ● ● ●

1.3 Využití nástroje Active Discovery
Zařízení | Detekce | ○ ● ●

1.4 Použití protokolu DHCP (Dynamic Host Configuration Protocol) k aktualizaci inventáře majetku podniku
Zařízení | Identifikace | ○ ● ●

1.5 Použití pasivního nástroje pro zjišťování majetku
Zařízení | Detekce | ○ ○ ●

1 2 3 4 5
Typ majetku | Funkce zabezpečení | ● ● ●

1= Typ majetku
2= Funkce zabezpečení
3= Implementační Skupina 1
4= Implementační Skupina 2
5= Implementační Skupina 3

BEZPEČNOSTNÍ OPATŘENÍ

2.1 Vytvoření a údržba inventáře softwaru
Aplikace | Identifikace | ● ○ ○

2.2 Zajistit aktuální podporu autorizovaného softwaru
Aplikace | Identifikace | ● ○ ○

2.3 Seznam ne-autorizovaného (zakázaného) softwaru
Aplikace | Reakce | ● ○ ○

2.4 Využití automatizovaných nástrojů pro inventarizaci softwaru
Aplikace | Detekce | ○ ○ ○

2.5 Seznam autorizovaného softwaru
Aplikace | Ochrana | ○ ○ ○

2.6 Seznam autorizovaných knihoven
Aplikace | Ochrana | ○ ○ ○

2.7 Seznam autorizovaných skriptů
Aplikace | Ochrana | ○ ○ ○

1 2 3 4 5
Typ majetku | Funkce zabezpečení | ● ● ●

1= Typ majetku
2= Funkce zabezpečení
3= Implementační Skupina 1
4= Implementační Skupina 2
5= Implementační Skupina 3

02 - Inventarizace a kontrola softwarového majetku

Bezpečnostní opatření celkem 7 | IG1 3/7 | IG2 6/7 | IG3 7/7

Aktivně spravovat (inventarizovat, sledovat a kontrolovat) veškerý software (OS a aplikace) v síti tak, aby byl nainstalován a mohl být spuštěn pouze autorizovaný software a aby byl nalezen neautorizovaný a nespravovaný software a bylo zabráněno jeho instalaci nebo spuštění.

Proč je tato kontrola CIS kritická?

Kompletní inventář softwaru je důležitým základem pro prevenci útoků. Útočníci neustále skenují cílové podniky a hledají zranitelné verze softwaru, které lze vzdáleně zneužít. Pokud například uživatel otevře škodlivou webovou stránku nebo přílohu pomocí zranitelného prohlížeče, může útočník často nainstalovat backdoor programy a boty, které mu poskytnou dlouhodobou kontrolu nad systémem. Útočníci mohou tento přístup využít také k dalšímu pohybu po síti. Jednou z klíčových obran proti těmto útokům je aktualizace a záplatování softwaru. Bez kompletního soupisu softwarových prostředků však podnik nemůže zjistit, zda má zranitelný software nebo zda nedochází k potenciálnímu porušování licencí.

I když záplata ještě není k dispozici, kompletní inventární seznam softwaru umožňuje podniku chránit se před známými útoky až do vydání záplaty.

Někteří sofistikovaní útočníci využívají tzv. zero-day exploity, které využívají dosud neznámé zranitelnosti, na které ještě nebyla vydána záplata od výrobce softwaru.

V závislosti na závažnosti exploitu může podnik zavést dočasná opatření na ochranu před útoky, dokud nebude vydána záplata.

Správa softwarových prostředků je také důležitá pro identifikaci zbytečných bezpečnostních rizik. Podnik by měl zkontrolovat inventář softwaru a zjistit, zda na podnikových zařízeních není provozován software, který není potřebný pro obchodní účely. Na firemní zařízení může být například z výroby nainstalován software, který představuje potenciální bezpečnostní riziko a nepřináší podniku žádný užitek. Je velmi důležité inventarizovat, pochopit, posoudit a spravovat veškerý software připojený k infrastruktuře podniku.

Věděli jste, že?

56 % firem ověřuje aktuální stav majetku pouze jednou ročně, zatímco 10-15 % pouze jednou za pět let. Pravidelná údržba majetku a inventáře je zásadní pro vedení přesné evidence. Můžeme vám pomoci se správou inventáře a kontroly softwaru.

03 - Ochrana dat

Bezpečnostní opatření celkem 14 | IG1 6/14 | IG2 12/14 | IG3 14/14

Vyvinout procesy a technické kontroly pro identifikaci, klasifikaci, bezpečné zpracování, uchovávání a likvidaci dat.

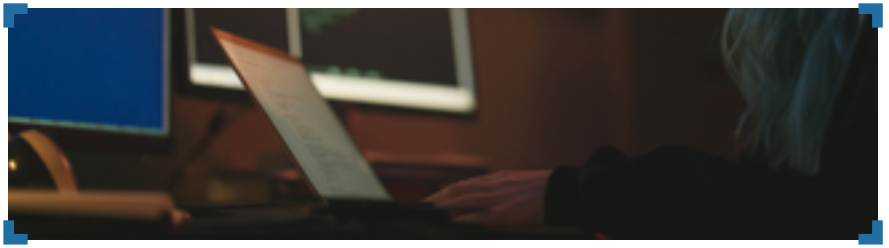
Proč je tato kontrola CIS kritická?

Data již nejsou obsažena pouze v rámci podniku; jsou v cloudu, na přenosných zařízeních koncových uživatelů, kde uživatelé pracují z domova a často jsou sdílena s partnery nebo online službami, které je mohou mít kdekoli na světě. Kromě citlivých údajů, které podnik uchovává a které se týkají financí, duševního vlastnictví a údajů o zákaznících, může existovat také řada mezinárodních předpisů na ochranu osobních údajů. Ochrana osobních údajů je stále důležitější a podniky se učí, že ochrana osobních údajů se týká vhodného používání a správy dat, nejen jejich šifrování.

Data musí být vhodně spravována po celou dobu svého životního cyklu.

Tato pravidla ochrany osobních údajů mohou být pro nadnárodní podniky jakékoli velikosti komplikovaná; existují však základy, které se mohou týkat všech.

Jakmile útočníci proniknou do podnikové infrastruktury, jedním z jejich prvních úkolů je najít a odcizit data. Podniky si nemusí být vědomy, že citlivá data opouštějí jejich prostředí, protože nemonitorují odliv dat.



Věděli jste, že?

78 % malých firem, které uchovávají cenná nebo citlivá data, je nešifruje, což hackerům usnadňuje přístup. V současné době jsou k dispozici nástroje a systémy, které mohou nákladově efektivně spravovat ochranu a šifrování dat v organizacích.

BEZPEČNOSTNÍ OPATŘENÍ

3.1 Zavedení a udržování procesu správy dat
Data | Identifikace | IG1 IG2 IG3

3.2 Vytvoření a udržování inventáře dat
Data | Identifikace | IG1 IG2 IG3

3.3 Konfigurace seznamů řízení přístupu k datům
Data | Ochrana | IG1 IG2 IG3

3.4 Pravidla uchovávání dat
Data | Ochrana | IG1 IG2 IG3

3.5 Bezpečná likvidace dat
Data | Ochrana | IG1 IG2 IG3

3.6 Šifrování dat v zařízeních koncových uživatelů
Data | Ochrana | IG1 IG2 IG3

3.7 Vytvoření a udržování systému klasifikace dat
Data | Identifikace | IG2 IG3

3.8 Dokumentace datových toků
Data | Identifikace | IG2 IG3

3.9 Šifrování dat na vyměnitelných médiích
Data | Ochrana | IG2 IG3

3.10 Šifrování citlivých dat při přenosu
Data | Ochrana | IG2 IG3

3.11 Šifrování citlivých dat
Data | Ochrana | IG2 IG3

3.12 Zpracování a ukládání dat v závislosti na citlivosti
Data | Ochrana | IG2 IG3

3.13 Nasazení řešení prevence úniku dat (DLP)
Data | Ochrana | IG3

3.14 Protokolování přístupu k citlivým datům
Data | Detekce | IG3

IAK MŮŽEME POMOCI

I VÁM MŮŽEME POMOCI

Pomůžeme vám zorientovat se ve složitém světě IT a kybernetické bezpečnosti, abyste mohli lépe chránit svá data a podnikání.

PROMLUVTE SI S NÁMI JEŠTĚ DNES!

(+420) 777-800-167

help@ict-group.cz

ict-group.cz

[ICT] GROUP

ZDROJE:

Pokud není uvedeno jinak, všechny statistiky pocházejí z následujících zdrojů:

- PurpleSec 2021 Cybersecurity Statistics
- Verizon 2019 Data Breach Investigations Report
- Cyber Rescue Alliance - Cyber Insights of 2021 Report
- FBI 2020 IC3 Annual Report

VAŠI, NEJEN [CYBER], PŘÁTELÉ Z

[ICT] GROUP

:-]

(+420) 777-800-167 | ict-group.cz