FYZICKÉ SE POTKÁVÁ S DIGITÁLNÍM

OSVĚDČENÉ POSTUPY V OBLASTI KYBERNETICKÉ BEZPEČNOSTI

IRON MOUNTAIN®

OSVĚDČENÉ POSTUPY V OBLASTI KYBERNETICKÉ BEZPEČNOSTI

Naru ení dat je pro firmy velkým problémem. To ukazuje také rychlý pohled na sou asná ísla.

- **Tém polovina** respondent studie, které se zú astnilo 4 200 evropských a amerických spole ností, zaznamenala v posledním roce narušení bezpe nosti dat[1].
- **Pr m rné náklady** na narušení dat se odhadují na 3,86 milionu dolar [2].

Riziko pro firmy ale nespo ívá pouze ve výši pokut. Hromadné aloby, pokles cen akcií, ztráta d v ry zákazník a poškození pov sti bude mít zna ný dopad také na zna ku spole nosti.

Existuje mnoho nástroj , které mohou firmy zavést ve snaze kybernetické útoky odvrátit. V tomto lánku se budeme zabývat širším pohledem. Jak m ete zavést osv d ené postupy kybernetické bezpe nosti v celé organizaci tak, abyste zachovali ochranu, integritu a dostupnost svých informa ních systém - a v p ípad narušení dokázali provést obnovu dat?

1. Bezpe nost na základ Hiscox/rizik: Stru ná zpráva o narušení dat za rok 2017
2. IBM / Ponemon Institute: náklady na narušení dat v roce 2018

MUSÍ SE KYBERNETICKOU BEZPEČNOSTÍ ZABÝVAT FIRMY VŠECH VELIKOSTÍ?

Hacker m na velikosti firmy nezále í. I kdy je pro n objem zákaznických dat velkých spole ností lákavý, p ístup k dodavatelským a platebním systém m menších firem jim také m e p inést zajímavé zisky.

V n kterých ohledech je problém pro malé a stední podniky ješt v tší, nebo mají omezené rozpo ty na bezpe nostní opat ení, a sou asn si nemohou dovolit být delší dobu offline.

PODÍVEJTE SE NA NAŠE VIDEO O KYBERNETICKÉ BEZPEČNOSTI

POCHOPENÍ PROSTŘEDÍ HROZEB

Víte, jaké druhy útok jsou mo né a jaký mohou mít dopad? Existuje mnoho typ hrozeb, které mohou vaši spole nost ovlivnit.

- Statistiky uvád jí, e **malware** - škodlivý software je i nadále nejv tší hrozbou, se kterou se musíme denn potýkat. Po íta ové viry, trojské kon a spyware jsou r zné formy malwaru. Sta í kliknout na nevinn vypadající odkaz a malware pronikne do po íta ových systém .

- **Ransomware** je stále populárn jší. Spole nost je kontaktována kybernetickým zlo incem, který tvrdí, e infikoval její data a uvolní je pouze po zaplacení výkupného. Spole nost neví, zda je tato hrozba skute ná, a neví, zda po zaplacení výkupného skute n dojde k uvoln ní dat, ale negativn bude ovlivn na tak jako tak, pakli e k napadení dat došlo.

- **Programy phishingu** se zam ují na u ivatele - d v ryhodn vypadajícími e-maily se hacke i sna í, aby jim u ivatelé zp ístupnili osobní a finan ní údaje.

Existuje mnoho dalších typ útok vedených r znými subjekty od národních stát p es organizovaný zlo in a po hackerské aktivisty. S trhem, který disponuje tém všemi typy dat, se bude podoba, rozsah a sofistikovanost kybernetických útok i nadále vyvíjet rychlým tempem.

Odborníci v této oblasti se obecn shodují, e není t eba plánovat, zda k narušení dat dojde, jako spíše kdy k tomu dojde. P íprava strategie pro prevenci útok je mimo ádn d le itá pro firmy jakékoliv velikosti.

POCHOPENÍ DAT, KTERÝMI DISPONUJETE

Víte, jaká data máte a pro ? Vystavujete riziku data, kterými byste ani nem li disponovat?

Porozum ní va im dat m je d le itým prvním krokem. **Efektivní správa a ochrana dat** v souladu s právními p edpisy je ivotn d le itá. To znamená pou ívat kvalitní správu dat, také chápat, jak vaše data proudí celou spole ností a zabezpe it je v ka dé fázi ivotního cyklu.

VYTVOŘENÍ STRATEGIE NA ZÁKLADĚ RIZIK

Mezi t i hlavní rizika, které je t eba ešit, pat í **riziko spojené s provozem spole nosti, riziko po kození dobré pov sti a riziko spojené s dodr ováním legislativy a p edpis .** P esto e neexistuje univerzální p ístup k ízení kybernetických rizik, je velmi cenné p izp sobit se zavedenému rámci kybernetické bezpe nosti, jako je ISO 27001 nebo americký Národní institut pro standardy (NIST).

Je vhodné poradit se s vaší pojiš ovnou o tom, který rámec bude pro vaši konkrétní situaci nejvhodn jší.

ZAHRNUTÍ PERSPEKTIVY CELÉ SPOLEČNOSTI

Kybernetická bezpe nost není jen o technologii. Spojuje odborné znalosti z oblasti IT, práva a bezpe nosti, aby vytvo ila funk ní rámec a dokázala hrozbám elit. Jde také o to, aby si ka dý jednotlivec ve spole nosti byl v dom toho, jak snadno se ho útok m e dotknout.

PODPORA PRACOVNÍ KULTURY S OHLEDEM NA BEZPEČNOST

Lidský prvek je p i vytvá ení bezpe ného prost edí rozhodující.

Slabina v systému asto nesouvisí s nekalým jednáním i nevinné kliknutí na špatné tla ítko m e umo nit p ístup kyberzlo inc do systému.

Zam stnanci musí vyhodnotit riziko a svou odpov dnost - klí em k uv domování si bezpe nosti jsou školení. Organizujte školení pro vaše zam stnance, která jim osv tlí význam d sledného jednání a dodr ování zásad bezpe nosti.

Sou asn je nutné ešit problémy spojené s nespokojenými zam stnanci nebo bývalými zam stnanci prost ednictvím:

- **monitorování chování** a projev zjevné nespokojenosti,
- **zavedení procesu** pro hodnocení a vy azování rizikových zam stnanc ,
- **implementace p ístupových oprávn ní** na základ rolí a omezování p ístupu k nejkriti t jším systém m a dat m.

PŘEČTĚTE SI VÍCE ▷

ROZVOJ SILNÉHO ŘÍZENÍ

Aby byla vaše strategie úsp šná, pot ebuje vaše spole nost pevné a stabilní vedení. To umo ní celé firm p izp sobit se kybernetické bezpe nosti, sní it dopad narušení dat a zajistit lepší alokaci a správu bezpe nostních zdroj .

Rámec silného ízení zahrnuje:

- zapojení vyššího vedení spole nosti,
- jednu osobu s jasnou odpov dností za kybernetickou bezpe nost,
- jasné zásady a postupy,
- silnou kulturu kyberbezpe nosti,
- plán odezvy.

BUDOVÁNÍ OBRANY DO HLOUBKY

Ochranná kontrolní opat ení mohou být narušena, proto je d le ité **pou ívat strategii** hloubkové obrany pro ochranu dat od vašich za ízení a po koncové. Pokud se úto ník dostane p es jednu linii obrany, máte nasazeny další linie.

Fyzické zabezpe ení by nap íklad m lo zabránit neoprávn ému p ístupu osob.

Sou asn by vedle pokro ilých nástroj na ochranu p ed hrozbami m la být pou ívána i tradi ní opat ení jako jsou kontroly sít a systému, firewally, prevence narušení a opat ení pro kontrolu p ístupu.

OBNOVA PO HAVÁRII: PLÁN TOHO NEJHORŠÍHO, CO MŮŽE NASTAT

Mnoho spole ností má plán obnovy po havárii a kontinuity provozu, ale historicky se jedná o p ípravu spíše na ne ekané události jako je povode nebo po ár. Kybernetické útoky, které vy adí firmu z provozu, však mají stejn katastrofální d sledky.

Zva te rozsah dopadu, který by úsp šný hackerský útok mohl mít na vaši firmu, a naplánujte, jak jej p ípadn zvládnout.

Mezi otázky, které by si va e spole nost m la polo it, pat í:

- Jak dlouho m e vaše firma p e ít výpadek a jaké kritické aplikace je t eba co nejrychleji obnovit? Menší firmy jsou náchyln jší, nebo útok m e ovlivnit i jejich finan ní toky.
- Kolik jste ochotni vynalo it na ešení výpadku? Nap íklad ukládání dat na více místech m e být dra ší, ale také ú inn jší.
- Zva ujete ka dý aspekt zálohování ve vašem fyzickém uspo ádání a po optická vlákna, která zajiš ují p ipojení sm rem do datového centra i ven?
- kolíte své zam stnance pro p ípad kybernetického útoku, testujete pravideln programy obnovy dat po útoku a zapojujete do t chto cvi ení své dodavatele a partnery?

Formální plán reakce usnad uje ešení a obnovu po útoku.

V praxi to znamená sestavení týmu pro reakci na mimo ádné incidenty a jeho pr b né školení. Nacvi ujte plán, provád jte teoretická cvi ení a plánujte, jak minimalizovat lidské chyby. P edtím, ne se kybernetické útoky stanou, m e být vhodné **anga ovat profesionální spole nost** zam enou p ímo na ešení t chto incident a uzav ít s ní spolupráci na základ SLA smlouvy.

- Vypracujte plán krizového ízení, který se bude týkat jak interních, tak externích zú astn ných stran tak, e jej bude mo né splnit a zachovat si d v ru.
- M jte plán i pro p ípad nouze, e b hem incidentu nebude fungovat b ná komunikace.
- V neposlední ad se ujist te, e máte kvalitní zálohu dat.

PODÍVEJTE SE NA NAŠE VIDEO O SESTAVENÍ PLÁNU OBNOVY PO HAVÁRII

VYTVÁŘÍTE PLÁN OBNOVY PO HAVÁRII A KONTINUITY PROVOZU?

PŘEČTĚTE SI VÍCE ▷

V PŘÍPADĚ NARUŠENÍ JEDNEJTE RYCHLE

Pr m rná doba odhalení narušení a reakce na n j je 197 dní a reakce na n j trvá v pr m ru dalších 69 dní[3]. ím rychleji zasáhnete, tím menší budou dopady a náklady. Spole nosti, které narušení dokázaly zvládnout za mén ne 30 dní, údajn ušet ily více ne milion dolar .

OZNAMTE NARUŠENÍ CO NEJDŘÍVE

Kdy navzdory veškerému plánování dojde k narušení bezpe nosti dat, oznamte to co nejrychleji, i kdybyste museli zprávu pozd ji aktualizovat. M ete tak výrazn ušet it na výši pokuty, kterou nakonec zaplatíte.

UDRŽUJTE SVŮJ PLÁN AKTUÁLNÍ

Pravideln se objevují nové technologie pro správu a analýzu dat. Firmy musí s tímto vývojem udr et krok a zahrnout technologie do plánování své kybernetické bezpe nosti.

M ete vyu ívat nové technologie jako je **um lá inteligence a machine learning** ke zlepšení své obrany, ale m jte na pam ti, e vaši protivníci budou d lat toté pro vylepšení svých útok .

Kybernetická bezpe nost bude i nadále hrou na ko ku a myš a je mimo ádn d le ité neustále udr ovat ostra itost.

VYBÍREJTE UVÁŽLIVĚ DATOVÉ CENTRUM

Pokud dáváte p ednost **outsourcingu svých systém** prost ednictvím datového centra zajišt ného t etí stranou, nezapome te, e jste zákazník a máte právo klást otázky týkající se fyzického zázemí, ale také postup a právních p edpis . Vyhovuje vám, komu je dovoleno do vašeho prost edí vstupovat? Máte smlouvu SLA, která zajiš uje, e budete informováni o jakémkoli narušení? Máte práva na audit? Jste si jisti tím, e poskytovatel spl uje legislativní rámce, jako nap íklad ISO 27001?

ZVAŽTE SVÉ DODAVATELE A PARTNERY

A u budete v kybernetické bezpe nosti jakkoli dob í, vaše firma není ostrov.

Jakékoliv spojení s t etími stranami hlídejte a sna te se s ním nakládat stejným zp sobem a pod obdobným dohledem jako uvnit své spole nosti i kdy to nebude v dy snadné.

3. IBM / Ponemon Institute: náklady na narušení dat v roce 2018

POKUD TO NEZVLÁDNETE SAMI, VYHLEDEJTE EXTERNÍ POMOC

Konzultant t etí strany zhodnotí vaše aktiva v míst jejich ulo ení a ur í, zda musí být zálohována. Provede také r zné modelace vašich potenciálních hrozeb.

Malé a stední firmy asto nejsou schopné dr et si bezpe nostního odborníka na plný úvazek. Najd te si místo toho partnera, který se n kolikrát ro n dostaví na kontrolu a odbornou konzultaci. M jte ho jako svého stálého poskytovatele i pro p ípad pohotovostního re imu, abyste jej m li k dispozici v p ípad útoku. Op t zde platí, e vaše pojiš ovna proti kybernetickým hrozbám vás pravd podobn ráda nasm ruje na n koho, komu d v uje.

ím více do programu investujete, tím lepší pravd podobn bude. Existuje mnoho firem, které projdou školeními, ale budou schopny také testovat u ivatele pro upevn ní a osvojení znalostí.

Pokud je mo nost spolupráce se t etí stranou mimo vaše mo nosti, existují **online organizace** jako SKA a IACPA. Také si m ete vyhledat šablony hodnocení hrozeb, které m ete pou ívat sami.

CHCETE ZÍSKAT VÍCE INFORMACÍ O KONTROLE, OCHRAN A OPTIMALIZACI D LE ITÝCH DAT SPOLE NOSTI V SOU ASNÉM HYBRIDNÍM INFORMA NÍM SV T ?

STÁHNĚTE SI E-BOOK ▷

O SPOLEČNOSTI IRON MOUNTAIN

Spole nost Iron Mountain Incorporated (NYSE: IRM), zalo ená v roce 1951, je celosv tovým lídrem v oblasti slu eb pro ukládání a správu informací. Spole nost Iron Mountain, které d v uje více ne 220 000 firem po celém sv t a která disponuje sítí nemovitostí o rozloze více ne 85 milion metr tvere ních ve více ne 1 400 za ízeních ve více ne 50 zemích, ukládá a chrání miliardy informa ních aktiv, v etn kritických obchodních informací, vysoce citlivých dat a kulturních a historických artefakt .

Spole nost Iron Mountain poskytuje ešení, která zahrnují bezpe né ukládání záznam , správu informací, digitální transformaci, bezpe nou likvidaci, ale také slu by datových center, cloudové slu by, um lecká úlo išt a logistiku. Pomáhá tak firmám sni ovat náklady a rizika, dodr ovat p edpisy, zajiš uje obnovu po haváriích a umo uje digitáln jší zp sob práce. Další informace naleznete na www.ironmountain.co.uk.

IRON MOUNTAIN®

CHRÁNÍME TO, ČEHO SI CENÍTE NEJVÍCE