MARSH

Byli jste napadeni Ransomware virem? Zde je, jak postupovat

Zrychlující se tempo technologických změn velmi dramaticky přetváří podnikatelské prostředí. Zároveň se neustále rozšiřuje škála kybernetických a technologických hrozeb, kterým podniky čelí a tyto hrozby působí stále větší ekonomické škody. Nejnovější průzkum společnosti **Marsh** využívající postřehy a zkušenosti z pojistných událostí v rámci kontinentální Evropy stejně jako zkušenosti a odborné znalosti společností **Wavestone** a **CMS** byl prezentován ve zprávě The Changing Face of Cyber Claims (Měnící se podoba kybernetických škod). Tato zpráva obsahuje praktické způsoby, jak řídit a zmírňovat kybernetická rizika a škody a mimo jiné zahrnuje **hloubkovou analýzu problematiky ransomwaru**.

Široké zkušenosti společnosti Marsh v tomto odvětví nám dovolují **nabídnout osvědčené postupy**, **jak pomoci firmám** lépe **porozumět**, **měřit a řídit** riziko ransomwaru, neboli vyděračského softwaru.

1. Porozumění: o čem se bavíme?

Cílem ransomwarových útoků je držet data napadené společnosti jako rukojmí (například jejich zašifrováním nebo hrozbou jejich zveřejnění) – s žádostí o zaplacení výkupného. Tento druh útoku se stal velmi populárním po celém světě, Evropu nevyjímaje. V roce 2019 jsme zaznamenali 100% nárůst těchto útoku napříč naším evropským portfoliem. Co je z našich zkušeností patrné:

Útokům se stále větší **četností** napomáhají nové typy ransomwaru a malwaru.

Provozní a finanční **závažnost** útoků prudce roste: požadavky na výkupné, související náklady a povozní prosto je rostou exponenciálně

Témata související s COVID-19 v podobě phishingových e-mailů cílí na zaměstnance pracující na dálku.

S narůstajícím počtem lidí pracujících v méně zabezpečených prostředích kybernetické bezpečnosti roste i úspěšnost útoků.

Na základě všech kybernetických pojistných událostí, které Marsh analyzoval, **67%** z nich bylo způsobeno **záměrným útokem**.

Počet pojistných událostí v souvislosti s ransomware se v průběhu roku 2019 **zdvojnásobil**

Délka **přerušení provozu u „jednoduchého" kybernetického útoku 1 týden pro úplné obnovní**

U „pokročilejšího" kybernetického útoku 3-4 týdny pro obnovení základní infrastruktury **6 týdnů** na re-import dat

* The Changing Face of Cyber Claims, 2020

MARSH & McLENNAN COMPANIES

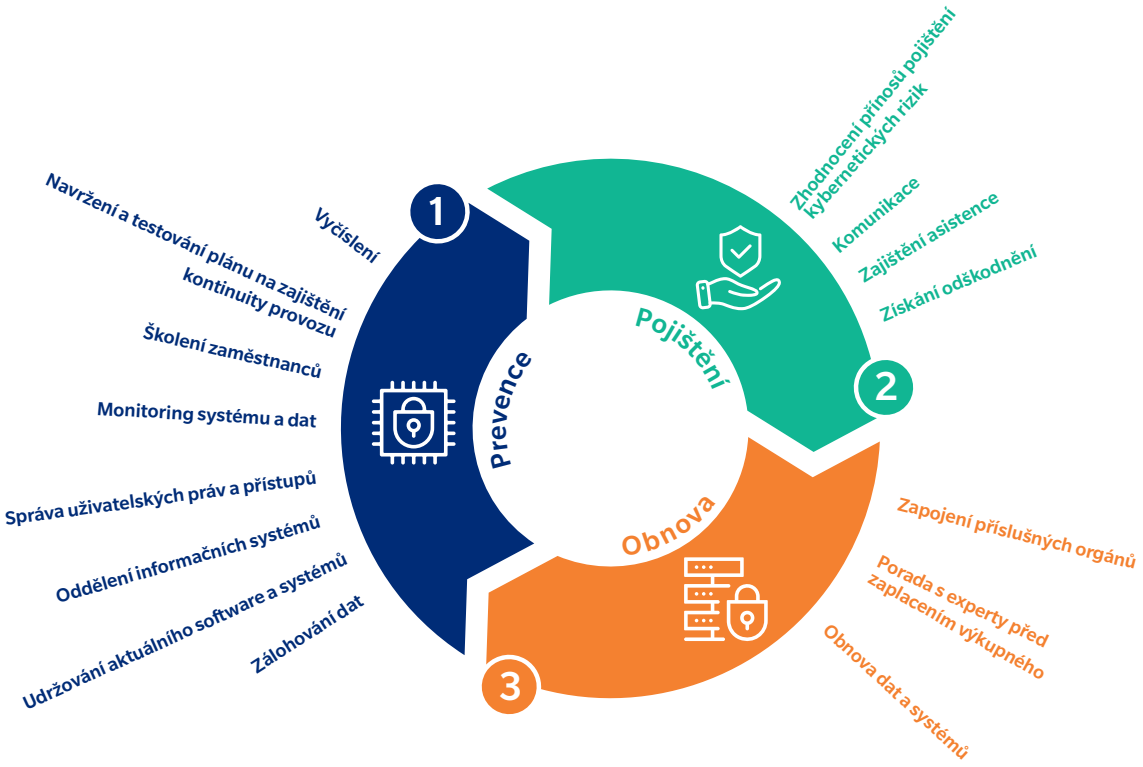
2. Změření: Jaká je cena takové události

Existují dva typy ransomwaru:

- **Necílený ransomware.** Náhodně rozeslán na miliony emailových adres, nejčastěji zaměřených na malé a střední firmy, či jednotlivé osoby. Mechanismus je jednoduchý a částka výkupného omezená (v průměru kolem 300€ v bitcoinech), ale na základě pouhého počtu obětí platících výkupné, je návratnost investice pro hackery obrovská.
- **Cílený ransomware.** Tyto útoky jsou méně časté a hackeři je pečlivě připravují, obvykle za použití sociálního inženýrství. Jsou zaměřeny na velké společnosti (s obratem >500 milionů €) a útočníci záměrně čekají na okamžik, kdy je cílová společnost nejcitlivější. V tomto případě jde o výkupné v řádech až několik desítek milionů eur.

3. Řízení: prevence, pojištění, obnova

Následující tipy mohou pomoct ochránit vaše aktiva před těmito velmi reálnými hrozbami:



PREVENCE

1. **Zálohování dat:** účelem většiny ransomwarů je zabránit vám v přístupu k vašim datům a vyžadování platby za jejich obnovení. Pro vaši společnost je zásadní pravidelné zálohování a udržování bezpečnosti záloh. Zároveň pravidelně testujte přesnost vašich záloh!
2. **Udržování aktuálního software a systémů:** váš informační systém obsahuje zranitelnosti a tyto slabé stránky využívají hackeři k šíření viru a šifrování vašich dat. Vyšší bezpečnosti dosáhnete pečlivým aktualizováním, to samé platí pro antivirový softwarem.
3. **Oddělené informační systémy:** některé části vašich dat a informačních systémů jsou kritičtější a citlivější než jiné. Jejich oddělením zajistěte, aby byly tyto prvky dobře chráněny proti snadnému přístupu ze strany hackerů.
4. **Správa uživatelských práv a přístupů:** ne každý zaměstnanec nebo partner by měl mít neomezený přístup do vašeho systému. Důsledný administrátor a „pořádek v domácnosti“ jsou zásadní.
5. **Monitoring systému a dat:** tímto nejdříve zjistíte jakékoliv neobvyklé chování ve vašich systémech – to znamená rychlejší reakci a vetší prevenci před poškozením.
6. **Školení zaměstnanců:** udělejte ze svých lidí tu nejlepší možnou obranu proti hrozbám. Ransomwarové útoky jsou často spuštěny skrze člena týmu, který otevře škodlivou přílohu nebo otevře škodlivou webovou stránku.
7. **Navržení a testování plánu na zajištění kontinuity provozu:** udělejte ze svých lidí tu nejlepší možnou obranu proti hrozbám. Ransomwarové útoky jsou často spuštěny skrze člena týmu, který otevře škodlivou přílohu nebo otevře škodlivou webovou stránku.
8. **Vyčíslení:** ransomware útok společnost destabilizuje. Nepřipravenost reagovat je cestou k selhání: nejlepším způsobem, jak s útoky zacházet je připravit se, včetně nastavení plánování a postupů reakce na incidenty.

POJIŠTĚNÍ

je pomoc v překování krize a podpora vašeho finančního zotavení

1. **Zhodnocení přínosů pojištění kybernetických rizik:** může vám poskytnout rychlou pomoc během útoku i po něm a zajistit náhradu vašich finančních ztrát.
2. **Komunikace:** po incidentu musí společnosti získat zpět důvěru svých klientů, zaměstnanců a partnerů. Odborníci vám pomohou znovu vybudovat silnou reputaci.
3. **Zajištění asistence:** mnoho firem nemá interní zdroje ani odborné znalosti, aby se dokázaly vypořádat s takovouto událostí. Specializovaní poskytovatelé služeb vám pomohou minimalizovat škody, a co nejrychleji vás dostanou zpět do podnikání. Forenzní analýza větších událostí vám pomůže pochopit, proč byl útok úspěšný, co bylo jeho hlavní příčinou a jaká vhodná opatření přijmout k úplnému zotavení. Zároveň vám pomůže být v budoucnu proti podobným útokům odolnější.
4. **Získání odškodnění:** pojištění kybernetických rizik zmírní finanční dopad události na pojištěnou společnost. V případě nejzávažnějších událostí může být poslední záchranou před „červenými čísly“ či bankrotem.

OBNOVA

zdokonalte se!

1. **Zapojení příslušných orgánů:** tyto vám mohou pomoci při vyšetřování a zotavování se z incidentu.
2. **Porada s experty před zaplacením výkupného:** V případě, že hackerům zaplatíte, neexistuje žádná záruka, že vám data opravdu rozšifrují – přeci jen jsou to podvodníci. Pokud uvidí, že jste ochotní platit, povede to nejspíš k dalším útokům od stejné skupiny nebo jiné a při dalším napadení budou daleko sofistikovanější.
3. **Obnova dat a systémů:** obnovte váš systém a data jen z důvěryhodných zdrojů a aktualizujte hesla. Je nezbytné zkontrolovat správnost a itegritu dat v zálohách a pečlivě zvolit stáří záloh, z nichž se bude systém obnovovat aby nedošlo k re-attacku (obnovení systému ze zálohy, do které již mohl proniknout virus).

Dále získávejte nejnovější informace, můžete si například přečíst naši zprávu *The Changing Face of Cyber Claims* pojednávající o tom, jak jsme se tento rok vypořádali s likvidacemi událostí.

O SPOLEČNOSTI MARSH

Marsh je přední mezinárodní pojišťovací makléř a poradce v řízení rizik. Za pomoci více než 35 000 kolegů z 130 zemí světa pomáháme našim klientům předvídat, vyčíslit a detailně se seznámit s celou škálou rizik, kterým čelí. V dnešním stále více nejistém globálním podnikatelském prostředí pomáhá společnost Marsh svým klientům prosperovat. S klienty všech velikostí spolupracujeme na definování, tvorbě a realizaci inovativních řešení s cílem lépe kvantifikovat a řídit rizika. Do každého vztahu se zákazníkem přinášíme bezkonkurenční kombinaci vysokého stupně specializace, duševního kapitálu, rizikového poradenství, pojišťovacího makléřství, alternativního financování rizika a řízení pojistných programů. Již od roku 1871 spoléhají klienti na společnost Marsh při poskytování důvěryhodného poradenství při zastupování jejich zájmů na trhu, zprostředkování informací o stále složitějším světě a při přetváření rizik na nové příležitosti růstu.

Pro více informací o pojištění kybernetických rizik a dalších možných řešení společnosti Marsh, navštivte naše stránky marsh.com nebo kontaktujte vašeho lokálního makléře Marsh.

JOSEF MAJER
Financial and Professional Lines Leader
Vinohradská 2828/151
130 00 Praha 3
josef.majer@marsh.com
+420 221 418 164 |
+420 730 573 931