RANSOMWARE

Bezpečnostní tipy pro malé a střední firmy

Digital Security Guide

ESET
Digital Security
Progress. Protected.

OBSAH

ÚVOD

RANSOMWARE JE NA VZESTUPU

Odhaduje se, že díky vysoké účinnosti vyděračských technik a novým distribučním kanálům ransomwaru skončily na účtech těchto technicky zdatných kyberzločinců stovky milionů dolarů, což některým z nich umožnilo vybudovat obchodní model ransomwaru jako služby (RaaS) a získat mnoho nových partnerů (zločinců s menšími dovednostmi a zkušenostmi).

Tyto zločinecké skupiny, které vytvářejí ransomware a provozují jej jako službu, v posledních několika letech provádějí útoky důmyslnějším a cílenějším způsobem, takže je těžší získat o těchto útocích přesnější informace. Kyberzločinci jsou stále agresivnější a vytrvale vyhledávají bezpečnostní slabiny – útočí na databáze, webové servery i chytré telefony. Útoky hrubou silou prostřednictvím protokolu vzdálené plochy (Remote Desktop Protocol, RDP) nebo DDoS útoky na webové stránky jsou jen zlomkem činnosti těchto pachatelů.

Předpokládá se navíc, že některé kyberzločinecké gangy začaly získávat zero-day zranitelnosti a nakupovat ukradené přihlašovací údaje, čímž se dále rozšiřuje okruh potenciálních obětí.

RANSOMWARE JAKO HROZBA PRO MALÉ A STŘEDNÍ FIRMY

Malé a střední firmy se stále častěji stávají cílem ransomwarových útoků. Proč? Protože tyto podniky shromažďují cennější údaje než domácí uživatelé a zároveň jim chybí propracovaná bezpečnostní opatření, která používají velké korporace nebo instituce.

Tyto skutečnosti jsou pro kyberzločince lákavé a zvyšují riziko ransomwarových útoků na malé a střední podniky.

Navíc manažeři malých a středních firem často nepovažují své firmy za potenciální cíle, nezálohují pravidelně svá důležitá data a nejsou na ransomwarové útoky dostatečně připraveni.

JAK FUNGUJE RANSOMWARE TECHNICKY?

Ransomwarový útok lze definovat jako pokus o vymáhání peněz po organizaci za to, že bude mít znovu přístup ke svým datům.

Zjistit, že jste se stali obětí, obvykle netrvá dlouho. Ransomware vás o své přítomnosti obvykle informuje brzy po napadení vašich zařízení – na obrazovce zobrazí oznámení s požadavkem výkupného, přidá textový soubor do napadených složek nebo změní přípony zašifrovaných souborů.

Typy ransomwaru

Ransomware blokující obrazovku

Tzv. screen locker blokuje přístup k zařízení pomocí zámku obrazovky a umožňuje používat pouze uživatelské rozhraní malwaru.

Ransomware uzamykající zařízení

Tzv. PIN locker mění PIN kód vašeho zařízení, čímž znepřístupní jeho obsah a funkce.

Ransomware šifrující pevný disk

Zašifruje spouštěcí záznam MBR (Master Boot Record) nebo klíčové struktury souborového systému a znemožní vám přístup k operačnímu systému.

Kryptografický ransomware

Zašifruje soubory na disku.

JAK FUNGUJE RANSOMWARE TECHNICKY?

Ransomware se rozšířil v průběhu pandemie COVID-19. Opakované lockdowny přinesly více phishingových e-mailů zaměřených na zaměstnance, kteří začali pracovat z domova a přistupovali k interním firemním systémům a službám pomocí protokolu RDP – ten se stal velmi oblíbeným prostředkem pro ransomwarový útok.

Kyberzločinci provozující ransomware jako službu (Ransomware as a Service, RaaS) navíc často zesilují útok tím, že nejprve získají přístup k jednomu počítači, odkud se přesunou na server a dále do sítě, přičemž teprve později se rozhodnou, zda ransomware použijí.

Kyberzločinci mohou také provádět útoky prostřednictvím „dodavatelského řetězce" (supply-chain attack), čímž získají přístup k celým IT ekosystémům. Ovládnutím oblíbených platforem MSP (Managed Service Provider) mohou zločinci ve velkém měřítku vypustit ransomware do mnoha sítí. Dalším trendem je, že se ransomwarové skupiny zaměřují na síťová úložiště (NAS), která poskytují data různým uživatelům a běžně se používají ke sdílení souborů a k zálohování.

JAK FUNGUJE RANSOMWARE PSYCHOLOGICKY?

Nátlak je klíčovou taktikou provozovatelů ransomwaru. Nátlak se zvyšuje, když jednotlivci nebo organizace skutečně přijdou o svou dobrou pověst, jsou svědky výpadků v podnikání nebo jsou dokonce právně či finančně postiženi.

S velkou pravděpodobností bude ze strany kyberzločinců následně docházet k manipulaci. Oběti jsou často napadeny na více místech, od DDoS útoků na webové stránky až po nepříjemné demonstrace přítomnosti zločinců v jejich síti. Může se jednat o následující nátlakové akce:

- Tiskový útok (print-bombing), při kterém je několika tiskárnám v síti přikázáno vytisknout výzvu k zaplacení výkupného – to ohrožuje schopnost managementu řídit interní a externí komunikaci.
- Získání přístupu k údajům o firemních zákaznících a jejich následné kontaktování nebo obvolávání (cold-calling) s dalším vyhrožováním a veřejným zostuzováním obětí, jejichž IT oddělení se mezitím snaží zmírnit dopady útoku.

ZVYŠUJÍCÍ SE TLAK NA OBĚTI

Kyberzločinci často násobí metody vydírání, aby získali požadovanou částku.

Dvojité vydírání

Tato metoda kombinuje šifrování dat s jejich exfiltrací. Kyberzločinci nejenže zabrání přístupu k cenným nebo důležitým souborům oběti, ale mohou je také zveřejnit nebo prodat jiným zločincům. Příkladem může být metoda zvaná doxing, kdy kyberzločinci získají citlivá data a vyhrožují, že je zveřejní, jestliže nebude zaplaceno další výkupné.

JAK FUNGUJE RANSOMWARE PSYCHOLOGICKY?

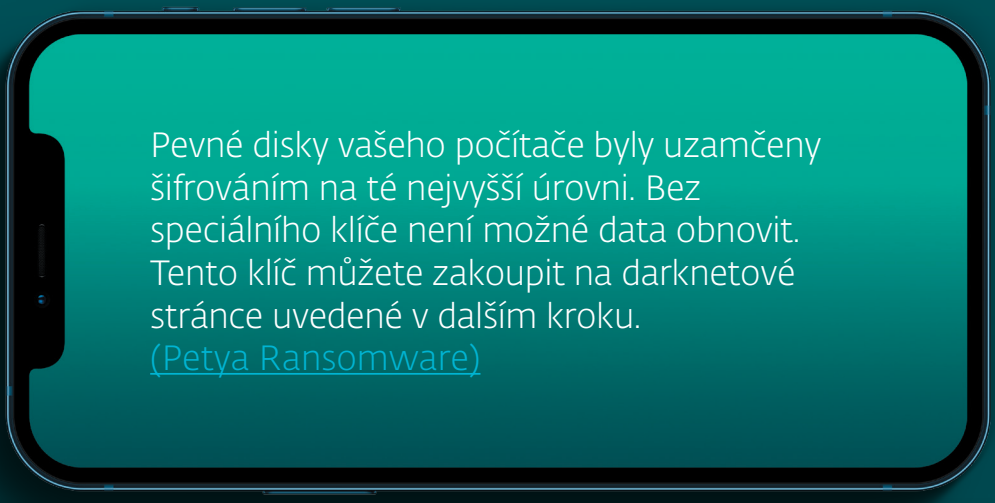
Trojité vydírání

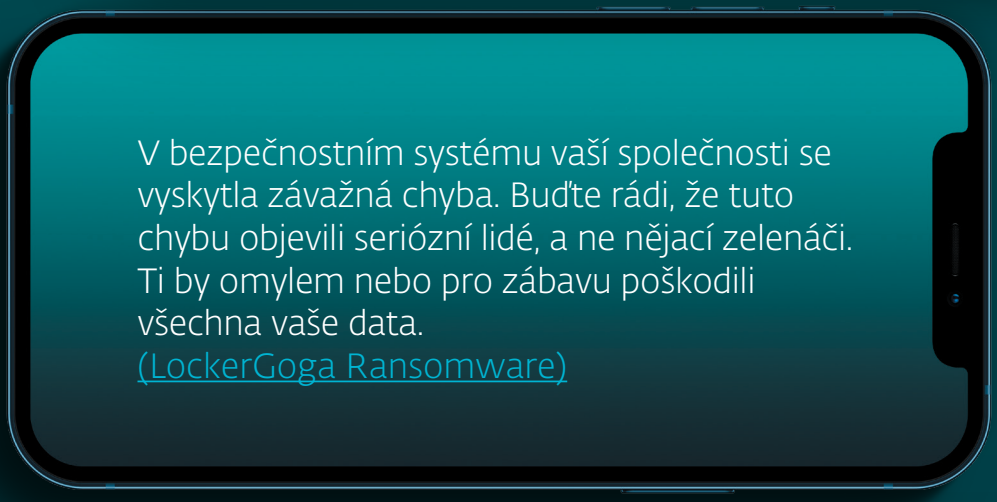
Někteří ransomwaroví útočníci kontaktují obchodní partnery nebo zákazníky napadené organizace, která nezaplatila výkupné, aby je informovali o tom, že v rámci ransomwarového útoku získali přístup také k jejich citlivým údajům. Útočníci dále požadují, aby tito partneři vyvíjeli nátlak na napadenou organizaci, aby zaplatila, a zabránili tak zveřejnění citlivých dat, nebo požadují platbu přímo od partnerů.

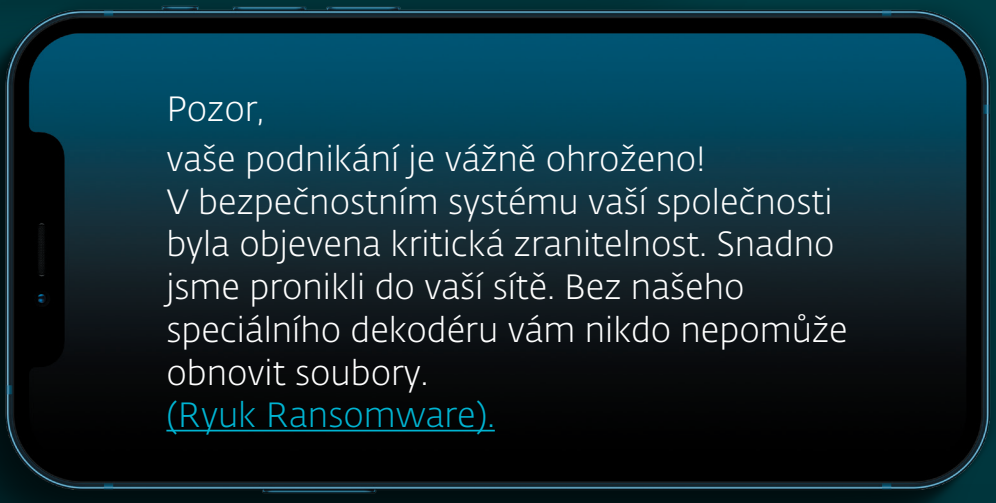
Jinými slovy, ransomware může nešťastný incident se škodlivým softwarem proměnit v psychologickou válku, jejímž cílem je donutit oběti jednat proti jejich vlastní vůli a zájmům. Tyto útoky nemusí pocházet z malwaru, zero-day exploitů nebo dlouhodobých kampaní. Mohou být jednoduše důsledkem špatných bezpečnostních postupů zaměstnanců, špatné konfigurace RDP a dalších nástrojů pro vzdálený přístup nebo mezer v postupech a procesech, a to jak v rámci vaší organizace, tak u poskytovatelů služeb a dalších subjektů v dodavatelském řetězci.

Bezpečnost je společná odpovědnost, a proto je třeba, aby školení o kybernetické bezpečnosti pro vaše zaměstnance byla aktuální a odrážela nejnovější trendy v oblasti kybernetických hrozeb. Jak se uvádí v bezplatném školení společnosti ESET o kybernetické bezpečnosti: „Počet incidentů se škodlivým softwarem, které musí vaše společnost řešit, můžete snížit, když vaši zaměstnanci budou seznámeni s tím, na co se zaměřit a čemu se vyhnout v případě phishingu a dalšího škodlivého obsahu."

Příklady výzev k zaplacení výkupného







RANSOMWARE VERSUS IT INFRASTRUKTURA

PROTOKOL RDP

Pokud zaměstnanci potřebují vzdálený přístup k firemním systémům, musí mít povolen protokol RDP. To vyžaduje, aby zaměstnanci i administrátoři přistupovali ke vzdálené ploše prostřednictvím vícefázového ověřování (MFA). Po ověření se mohou zaměstnanci k těmto systémům bezpečně připojit.

infobox

K čemu mohou organizace používat protokol RDP?

1) Ke správě programů spuštěných na serveru, například webových stránek nebo databází.

2) Pro vzdálený přístup k firemním desktopům nebo virtuálním počítačům s přístupem k datům, která jsou mimo firemní síť nepřístupná. Znamená to, že pokud se k takovým systémům přistupuje prostřednictvím protokolu RDP, není nutné citlivá data z interních serverů ohrožovat.

RANSOMWARE VERSUS IT INFRASTRUKTURA

Proč je odhalení vnějších systémů a jejich zneužití tak jednoduché?

- Zranitelné systémy RDP lze snadno najít (např. pomocí specializovaných vyhledávačů, jako je Shodan).
- Pokud mají systémy RDP špatnou konfiguraci, útočníci do nich mohou snadno proniknout.
- Nástroje a techniky pro eskalaci oprávnění a získání administrátorských práv na napadených systémech RDP jsou všeobecně známé a dostupné.

71 miliard

Počet detekcí útoku prostřednictvím RPD mezi lednem 2020 a červnem 2021 podle měření společnosti ESET.

Celkový počet otevřených portů 3389 (výchozí port pro RPD) nalezených vyhledávačem Shodan.io

Více než 4 miliony

Infografika

Detekce útoků hrubou silou prostřednictvím RDP v průměru za sedm dní

Zatímco v první polovině roku 2020 došlo k výraznému nárůstu těchto útoků, v roce 2021 byl jejich počet dosud nejvyšší. Ve srovnání s prvním pololetím roku 2020 zaznamenala společnost ESET v prvním pololetí roku 2021 šestinásobný nárůst útoků prostřednictvím RDP. Útoky tohoto typu navíc mohou unikat detekčním metodám, což má za následek méně zjištěných údajů a menší povědomí o hrozbách.

RANSOMWARE VERSUS IT INFRASTRUKTURA

JAK CHRÁNIT FIRMU PŘED RANSOMWARE ÚTOKY PROSTŘEDNICTVÍM PROTOKOLU RDP

- Zaveďte pravidla pro zabezpečení vzdáleného přístupu. Přístup k RDP by měl být směrován přes VPN (virtuální privátní síť) a zabezpečen pomocí vícefázového ověřování (MFA) nebo omezen na stanovené role a na konkrétní systémy, které jsou bezpečně nakonfigurovány, okamžitě záplatovány, neustále monitorovány, náležitě chráněny firewallem a pravidelně zálohovány.
- Ujistěte se, že všichni tato pravidla dodržují, a zároveň buďte připraveni na útok, který by navzdory těmto pravidlům mohl nastat.
- Proveďte soupis zařízení, která jsou připojena k internetu. Na základě našeho průzkumu je následující scénář poměrně obvyklý: organizace je napadena prostřednictvím zařízení připojeného k internetu, o kterém bezpečnostní pracovníci před útokem nevěděli.
- Nedovolte dodavateli nebo zaměstnanci, aby do sítě vaší organizace připojil fyzický nebo virtuální server, pokud není tento server bezpečně nakonfigurován. Konfigurace musí proběhnout před spuštěním serveru do ostrého provozu, zejména pokud je na serveru spuštěn protokol RDP pod účtem správce domény.
- Zdokumentujte, která zařízení s přístupem k internetu mají povolený vzdálený přístup, a rozhodněte, zda je tento přístup nezbytný. Pokud je přístup skutečně nezbytný, vyžadujte dlouhá hesla pro účty, které takový přístup budou mít. Zjistěte, zda není možné omezit přístup těchto zařízení pouze na interní síť a přistupovat k nim vzdáleně pomocí VPN.
- Pokud je třeba k systému přistupovat z veřejného internetu prostřednictvím protokolu RDP a není možné použít síť VPN, používejte vícefázové ověřování (MFA), abyste se nemuseli spoléhat pouze na hesla. Použijte takové řešení MFA, které není založeno na SMS. Zločinci mají spoustu způsobů, jak obejít ověřování pomocí SMS. V případě, že se spoléháte pouze na hesla, nastavte limit tří neplatných pokusů o přihlášení, po jehož překročení nebude po stanovenou dobu uznán žádný pokus o přihlášení: například tři minuty.
- Zabezpečte a aktualizujte všechna vzdáleně přístupná zařízení. Kromě identifikace a odstranění všech bezpečnostních zranitelností se ujistěte, že byly odstraněny nebo zakázány služby a součásti, které nejsou nezbytné, a že nastavení jsou nakonfigurována s ohledem na maximální zabezpečení.

RANSOMWARE VERSUS IT INFRASTRUKTURA

E-MAIL

Někteří zločinci stále používají přílohy e-mailů k instalaci malwaru, který nakonec vede k ransomwarovému útoku.

E-mail mohou útočníci použít také k doručení downloaderů, které nainstalují malware do počítače příjemce e-mailu, nebo k ovládnutí zařízení v síti vaší organizace. Na základě toho se mohou pokusit ukrást cenná data a zašifrovat soubory v celé organizaci a následně požadovat velmi vysoké výkupné, podobně jako v případě cílených ransomwarových útoků prostřednictvím RDP.

E-mail je také jedním z hlavních prostředků pro botnety, jako jsou Trickbot, Qbot a Dridex, které používají dokumenty Microsoft Office se škodlivými makry pro počáteční průnik následovaný ransomwarovým útokem.

Zdůrazněte zaměstnancům, že by měli podezřelé zprávy a přílohy ihned nahlásit technickému oddělení nebo bezpečnostnímu týmu. Včasné varování může organizaci pomoci vyladit filtry spamu a obsahu e-mailových zpráv a posílit firewally a další obranné prvky.

příklad

Od jednoho e-mailu k nepoužitelným elektronickým dveřím v hotelu

Ransomware nemusí šifrovat jen data v počítači. Ředitel čtyřhvězdičkového hotelu v rakouských Alpách dostal e-mail s ransomwarem, který byl maskován jako účet od společnosti Telekom Austria. Po kliknutí na odkaz v e-mailu přestaly v jeho hotelu fungovat elektronické dveře a on nemohl hostům vydat přístupové karty. Rozhodl se proto zaplatit výkupné ve výši dvou bitcoinů.

Následně byl tento hotel napaden ještě třikrát. To jen dokazuje, že zaplacením výkupného dáváte zločincům najevo svou ochotu platit a zvyšujete tak šanci, že v budoucnu zaútočí znovu.

Zdroj: BBC

RANSOMWARE VERSUS IT INFRASTRUKTURA

DODAVATELSKÝ ŘETĚZEC

Dodavatelský řetězec je síť vztahů mezi společností a jejími dodavateli za účelem výroby a distribuce určitého výrobku nebo služby. Útok na dodavatelský řetězec v kterémkoli z jeho bodů bude mít důsledky pro celý řetězec.

Ačkoli jsou útoky na dodavatelský řetězec spíše digitální než fyzické, mají podobně škodlivé účinky. Napadením jednoho z účastníků dodavatelského řetězce mohou zločinci získat neomezený a těžko odhalitelný přístup k datům obchodních partnerů a zákazníků.

příklad

Co se může stát v případě útoku na dodavatelský řetězec?

V roce 2017 společnost ESET zjistila že zločinci k šíření malwaru NotPetya nebo DiskCoder.C využívají legitimní účetní software. Útočníci pronikli na aktualizační servery softwarové společnosti a do legitimních aktualizačních souborů aplikací přidali vlastní kód. Když uživatelé účetního softwaru instalovali aktualizaci programu, instalovali zároveň zadní vrátka malwaru, čímž otevřeli cestu k nejničivějšímu kybernetickému útoku v historii.

Zdroj: WeLiveSecurity

Rostoucí intenzitu útoků na dodavatelský řetězec dokládá i počet publikovaných výzkumných článků společnosti ESET, které o tomto typu útoku pojednávají. V období od listopadu 2020 do února 2021 byly zaznamenány čtyři případy útoků na dodavatelský řetězec, které byly objeveny jen díky společností ESET, což je v porovnání s předchozími lety poměrně vysoký počet.

Obrana proti tomuto typu útoku spočívá ve sledování aktualizací a záplat softwaru, používání programů pro ochranu koncových bodů, případně využití řešení EDR a poučení zaměstnanců o tom, jak mají nakládat s nevyžádanými e-maily, které je nabádají k návštěvě neznámých webových stránek.

RANSOMWARE VERSUS IT INFRASTRUKTURA

DALŠÍ ZRANITELNOSTI

Zatímco běžní kyberzločinci využívají známých i neznámých zranitelností, zero-day útoky jsou převážně doménou skupin označovaných jako pokročilá trvalá hrozba (Advanced Persistent Threat, APT) a státem sponzorovaných skupin. Tento typ útoku je noční můrou správců zabezpečení i majitelů firem.

Téměř všichni dodavatelé kybernetické bezpečnosti stále detekují aktivitu exploitu EternalBlue (2017) a spoustu jeho variant, stejně jako pokračující útoky založené na protokolu SMBv1 pro sdílení souborů v systému Windows. Dlouhá životnost zranitelností a hrozeb, jako je WannaCryptor (neboli WannaCry), obvykle souvisí s nedostatečnou aktualizací a správou záplat ve firmách a institucích.

A konečně, sítě VPN vyžadují také proaktivní přístup správců IT, kteří by měli aktualizovat produkty kybernetické bezpečnosti. Důraz na včasné aktualizace by mělo doprovázet používání vícefázového ověřování při přihlašování ke službám VPN. Pokud vznikne podezření na zneužití přístupových údajů, měly by organizace usilovat o resetování všech uživatelských účtů.

příklad

Útoky prostřednictvím Microsoft Exchange Serveru

V březnu 2021 společnost Microsoft urychleně vydala mimořádné aktualizace, které řešily čtyři zero-day zranitelnosti Microsoft Exchange Serveru verze 2013, 2016 a 2019. Zločinci zneužívali tyto zranitelnosti k přístupu k lokálním Exchange serverům, což jim umožňovalo krást e-maily, stahovat data a kompromitovat počítače malwarem pro dlouhodobý přístup do lokálních sítí.

Zdroj: WeLiveSecurity

STRATEGIE OBRANY PROTI RANSOMWARU

SEGMENTACE CLOUDU A SÍTĚ

Pokud se jakýkoli typ ransomwaru dostane do vaší organizace, je pravděpodobné, že se pokusí rozšířit na co největší počet počítačů a ovlivnit všechny operace vaší společnosti.

Z hlediska obrany je strategicky výhodné omezit počet počítačů, na které se útočník může dostat z jednoho vstupního zařízení. Tuto strategii je možné realizovat různými způsoby – zejména segmentací sítě.

Oblíbenou strategií architektury systému se v posledních letech stal přesun dat do cloudu. Cloud však neposkytuje automatickou imunitu proti ransomwarovým útokům. Ve skutečnosti jsou nízké náklady a relativní snadnost, s jakou lze v cloudu zajistit nové servery a připojit je ke zbytku sítě organizace, důvodem, proč se z cloudu stala úrodná půda pro zločince. Je proto zřejmé, že jakékoli využití cloudu musí být řádně autorizováno a bezpečně nakonfigurováno. Stejně jako všechny ostatní systémy musí mít i ty v cloudu správně nastavený systém zálohování a obnovy dat.

STRATEGIE OBRANY PROTI RANSOMWARU

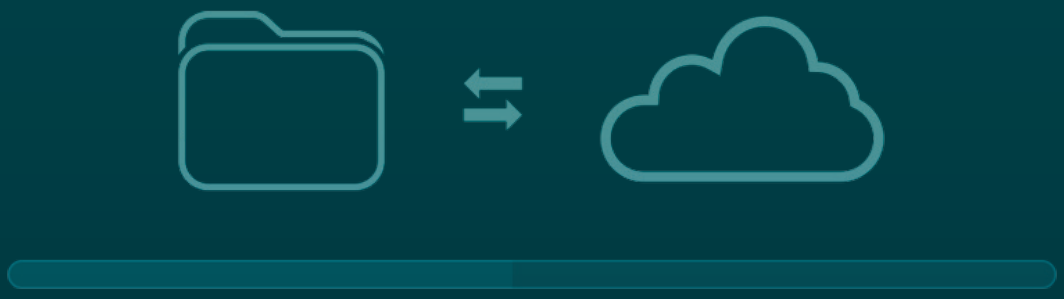
ZÁPLATOVÁNÍ (PATCHING) A ZÁLOHOVÁNÍ (BACKUP)

Záplatování a zálohování jsou jedny z nejdůležitějších činností pro správu systémů. Hrají zásadní roli při ochraně před ransomwarovými útoky.

Záplatováním systémů se uzavřou potenciální cesty útoku a zabrání se proniknutí ransomwaru do organizace. Pokud se tak stane, lze záplatováním snížit možné škody. Správné zálohování a program obnovení dat jsou důležitým obranným mechanismem, který má zásadní význam při obnově dat, pokud se do vaší organizace dostane ransomware.

To může být mnohem složitější, než se zdá. Proč? Záplaty a aktualizace je třeba před nasazením otestovat. Některé systémy vaší organizace mohou mít softwarové závislosti, které se mohou aktualizací na nejnovější verzi aplikace nebo operačního systému narušit.

Mějte na paměti, že některé útoky ransomwaru jsou prováděny po delší dobu, během níž může být zálohován také ransomware. To ohrožuje možnost snadného obnovení. Proto zálohování není obranou s jednorázovým nastavením. Zálohování je třeba průběžně sledovat a proces obnovy pravidelně testovat.



STRATEGIE OBRANY PROTI RANSOMWARU

Pro zálohování a obnovu dat už dnes existuje spousta možností – zejména cloudová úložiště, ať už vzdálená, lokální nebo hybridní. Zároveň je však také více dat z více zdrojů, která je třeba zálohovat. Pokud nemáte komplexní strategii zálohování, vždy existuje možnost, že šiřitelé ransomwaru najdou to jediné zařízení, jehož zálohování jste zanedbali.

Podle odborníků na zálohování ze společnosti Xopero, člena ESET Technology Alliance, komplexní zálohování zahrnuje data a stav systému na všech koncových bodech, serverech, poštovních schránkách, síťových discích, mobilních zařízeních a virtuálních počítačích. Při ochraně před ransomwarem je však třeba být před některými skutečnostmi na pozoru.

Pokud je například úložiště „stále zapnuté", může být jeho obsah lehce napadnutelný ransomwarem stejně jako místní úložiště nebo jiná úložiště připojená k síti.

infobox

Jak zabránit šíření ransomwaru

Vyberte si externí úložiště, které:

- Není trvale online.
- Chrání zálohovaná data před automatickou a „tichou modifikací" nebo přepsáním škodlivým softwarem, když je vzdálené zařízení online.
- Chrání starší zálohy dat před ohrožením, takže i když dojde k napadení nejnovějších záloh, můžete alespoň některá data získat zpět, včetně dřívějších verzí aktuálních dat.
- Chrání zákazníka tím, že stanoví právní a smluvní povinnosti poskytovatele v případě, že poskytovatel například ukončí obchodní činnost.

Nepodceňujte užitečnost médií s jednorázovým zápisem pro zálohování dat. Soubory uložené na nepřepisovatelných médiích jsou imunní vůči ransomwarovým útokům.

REAKCE NA RANSOMWARE

I když jste nepodcenili nebezpečí ransomwaru a zavedli jste všechna potřebná preventivní opatření, vaše organizace musí být připravena reagovat na ransomwarový útok, kterému se podaří prolomit vaši obranu. Nabízíme praktický přehled, který může být užitečný při plánování reakce na ransomwarový útok.

infobox

Rozumí vaši zaměstnanci bezpečnostním zásadám a předpisům?

Otázky k diskusi ve společnosti:

- Komu mají zaměstnanci hlásit podezření na ransomware?
- Jaké jsou zásady společnosti ohledně placení výkupného?
- Jaké kroky je organizace povinna podniknout v případě porušení ochrany osobních údajů?
- Kdo smí platit výkupné nebo o něm vyjednávat?
- Jaké předpisy má společnost pro deaktivaci postižených zařízení?
- Kdo o tom rozhoduje? Deaktivací zařízení se smažou potenciální důkazy uložené v paměti, což může být v rozporu s předpisy.

Problémy, kterým je třeba se vyhnout:

- Zaměstnanci nehlásí podezření na ransomware ze strachu z postihu.
- Správci sítí raději zaplatí výkupné, protože je to jednodušší než obnovovat systémy ze záloh.
- Neoprávněné zveřejňování informací o skutečných nebo domnělých ransomwarových útocích.

REAKCE NA RANSOMWARE

PLÁN OBNOVY

Je dobré mít v krizovém plánu alespoň jeden scénář pro případ ransomwarového útoku a projít si ho na poradě s příslušnými pracovníky, včetně vedoucích.

Můžete tak odhalit nedostatky v plánech na zálohování a obnovu a lépe předvídat, co nastane, když kvůli zašifrování nebudete mít přístup k základním službám jako jsou e-maily, VoIP telefony a přístup k internetu.

Příklad efektivního plánu reakce na útok a plánu na obnovu

1) Při prvních náznacích útoku uvědomte pověřené pracovníky.
2) Izolujte a analyzujte postižená zařízení.
3) Pokud není možné postižená zařízení izolovat, pořiďte obraz systému a paměti a poté je vypněte, abyste zabránili dalšímu šíření ransomwarovému útoku.
4) Jakmile je útok potvrzen, zapojte tým pro řešení mimořádných událostí nebo krizových situací.
5) Upozorněte právního zástupce.
6) Kontaktujte obchodní partnery, kteří vám mohou pomoci.
7) Připomeňte zaměstnancům pravidla pro sociální sítě a média, abyste udrželi kontrolu nad komunikací směrem k veřejnosti.
8) Posuďte rozsah a specifika ransomwarového útoku (např. zjistěte, zda je k dispozici šifrovací klíč v poznámce od vyděrače).
9) Kontaktujte orgány činné v trestním řízení.
10) Připravte PR prohlášení k situaci.
11) Pokud byly soubory zašifrovány, zjistěte, zda je lze obnovit ze zálohy.
12) Informujte zaměstnance o stavu situace.
13) V případě potřeby postupujte podle plánu zajištění kontinuity provozu.

REAKCE NA RANSOMWARE

14) Správce IT by měl shromažďovat příslušné protokoly a případné indikátory kompromitace, jako jsou binární soubory, žádosti o výkupné, IP adresy, záznamy v registrech nebo jiné soubory.

15) Zdokumentujte počáteční vyšetřování útoku a kroky podniknuté k nápravě.

PROČ BYSTE NEMĚLI PLATIT VÝKUPNÉ

Zaplacení zločincům, kteří zašifrovali vaše soubory, v žádném případě nezaručuje, že získáte dešifrovací klíč. Existuje řada důvodů, proč po zaplacení nemusíte získat své soubory zpět:

1) Některá data mohla být při šifrování poškozena, a proto je nelze obnovit.
2) Poskytnutý nástroj pro dešifrování může být spojen s jiným škodlivým softwarem, nemusí fungovat správně nebo může být mnohem pomalejší než obnova ze zálohy.
3) Proces doručení dešifrovacího klíče může selhat.
4) Útočník může jednat se zlým úmyslem a nemusí mít v plánu poskytnout dešifrovací klíče.
5) Placení výkupného může být nezákonné. Například v říjnu 2020 prohlásil Úřad pro kontrolu zahraničních aktiv (OFAC) Ministerstva financí USA, že zprostředkování plateb osobám, organizacím, režimům a v některých případech i celým zemím, které jsou na sankčním seznamu, je nezákonné.

Navíc existují etické důvody, proč požadované výkupné nezaplatit. Pokud to totiž uděláte, ...

... schvalujete obchodní model, který stojí za trestným činem.
... podporujete další trestnou činnost.
... umožňujete ransomwarovým gangům hledat zero-day zranitelnosti a vyvíjet nové útoky.
... můžete být v budoucnu vystaveni dalším útokům a dalšímu vydírání.

infobox

Typické argumenty pro zaplacení výkupného

„Je to levnější než obnova ze záloh."

Pokud je toto tvrzení založeno pouze na výpočtu času a práce, může být technicky správné, nicméně zaplacení výkupného je z výše uvedených důvodů velmi chybné. Také odstranění aktivního ransomwaru pomocí bezpečnostního softwaru není v žádném případě totéž jako obnovení dat. Odstranění ransomwaru a následné rozhodnutí zaplatit znamená, že data již nemusí být možné obnovit ani ve spolupráci se zločinci, protože dešifrovací mechanismus je často součástí malwaru.

„Zašifrované informace nemůžeme obnovit ze záloh."

Důvodem může být neexistence, neúplnost nebo poškození záloh. Existují však i jiné možnosti než zaplatit. Nejprve se obraťte na dodavatele bezpečnostního softwaru a zjistěte, zda není k dispozici dešifrovací nástroj, který by umožnil obnovu bez placení výkupného.

BUDOUCNOST RANSOMWARU

Ransomware využívá závislosti organizace na technologiích. Proto lze očekávat, že se ransomware bude v budoucnu dále vyvíjet, pokud nedojde k nepředvídatelným změnám v globální politice a ekonomice.

Na základě našich zkušeností se škodlivým kódem už od konce 80. let můžeme říct, že malware se má tendenci vyvíjet podle následujícího scénáře:

- Jsou objeveny zranitelnosti nové technologie nebo softwaru a diskutuje se o jejich potenciálním zneužití k trestné činnosti.
- Pokusy o kriminální zneužití nejnovějších technologií jsou zpočátku vzácné, protože zločinci snadněji vydělávají na zavedených strategiích.
- Začne se usilovně pracovat na opravě a zmírnění těchto zranitelností.
- Pokud nedojde k rozsáhlému zneužívání zločinci, úsilí vyvíjené na opravu a zmírnění zranitelností ztrácí na síle.
- Méně kvalifikovaní zločinci nakonec zjistí, že tato „nová" technologie je zralá pro zneužití.
- Objevuje se nový trend v oblasti malwaru.

Tento scénář vývoje ransomwaru má pro malé a střední podniky řadu důsledků. Je na čase začít se těmito potenciálními hrozbami zabývat v rámci vaší strategie řízení rizik a plánování.

Začněte se zajímat o zařízení, za která by někdo mohl vyžadovat výkupné: zařízení internetu věcí, SOHO routery, roboty, řídicí systémy a autonomní systémy. Sledujte zprávy o zranitelnostech těchto zařízení a sledujte jejich záplaty a aktualizace firmwaru.

Segmentujte také zařízení internetu věcí a další nové technologie.

ZÁVĚR

Vzhledem k tomu, že peníze a motivace jsou většinou na straně ransomwarových gangů, je pro správce IT, odborníky na zabezpečení i vedoucí pracovníky nezbytné poučit se z příběhů o napadení a z analýz, o nichž denně informují média. Opakovaně se ukazuje, že dodržování pravidel, správná konfigurace a silná hesla v kombinaci s vícefázovým ověřováním jsou rozhodujícími prvky v boji proti ransomwaru.

Proti zero-day zranitelnostem, botnetům, malspamu (spamu obsahujícímu malware) a dalším technicky pokročilým technikám jsou zapotřebí další bezpečnostní technologie. Mezi tyto technologie patří vícevrstvá ochrana koncových bodů, která dokáže detekovat a blokovat hrozby přicházejících v e-mailech, prostřednictvím webových odkazů, protokolu RDP a dalších síťových protokolů. Dále jde o nástroje pro detekci a reakci koncových bodů, které monitorují, identifikují a izolují jakékoli náznaky škodlivých aktivit v prostředí organizace.

Zabezpečte své koncové body před ransomwarem s řešeními ESET. Pro další informace nás kontaktujte na adrese obchod@eset.cz.

O SPOLEČNOSTI ESET

Společnost ESET® již více než 30 let vyvíjí špičkový software a služby v oblasti IT bezpečnosti, které chrání firmy, kritickou infrastrukturu a spotřebitele po celém světě před stále sofistikovanějšími digitálními hrozbami. Od zabezpečení koncových bodů a mobilních zařízení až po detekci a reakci koncových bodů, stejně jako šifrování a vícefázová autentizace, vysoce výkonná a snadno použitelná řešení ESET nenápadně chrání a monitorují 24/7. Aktualizují obranu v reálném čase, aby uživatelé byli v bezpečí a firmy fungovaly bez přerušení. Vyvíjející se hrozby vyžadují vyvíjející se společnost zaměřenou na kybernetickou bezpečnost, která zajišťuje bezpečné používání digitálních technologií. Za tím stojí výzkumná a vývojová centra společnosti ESET po celém světě, která pracují na naší společné budoucnosti. Pro více informací navštivte www.eset.com nebo nás sledujte na LinkedIn, Facebook, a Twitter.

Digital Security
Progress. Protected.