Synology

Ochrana organizace před ransomwarem

Podle předpovědí budou útoky ransomwarem v roce 2023 stát organizace v USA celkem 8 biliónů USD.[1] Pro zmírnění dopadu ransomwaru a dalších forem kybernetické zločinnosti jsou důležité plány ochrany dat s možnostmi jejich rychlého obnovení.

Date 13. říj 2023

Zálohy: poslední obranná linie při havárii

Pokud dojde ke ztrátě dat v důsledku záměrného odstranění nebo změny, můžete důležitá data obnovit ze záloh a předejít tak nákladným odstávkám. Řešení pro ochranu dat Synology umožňují navrhnout strategii zálohování pro vaši kompletní infrastrukturu IT.

Kompletní ochrana

Chraňte koncové body i primární zálohy a vytvářejte pro svoje data více vrstev záchranných sítí.

Rychlé obnovení

Možnosti okamžitého obnovení umožňují v případě havárie zkrátit odstávku na minimum.

Neměnné úložiště

Předcházejte neoprávněným změnám dat a snímků.

Zálohování bez licencí

Zálohovat můžete tolik dat, kolik vaše úložiště dovolí – bez omezení nebo skrytých poplatků.

Centralizovaná ochrana před útoky ransomwarem

Konsolidujte zálohy ze všech svých pracovních stanic, serverů, virtuálních počítačů a cloudových aplikací. Technologie deduplikace dat a přírůstkového zálohování umožňuje optimalizovat spotřebu úložiště a předcházet omezení šířky pásma. https://www.synology.com/dsm/solution/infrastructure

Fyzické pracovní zátěže

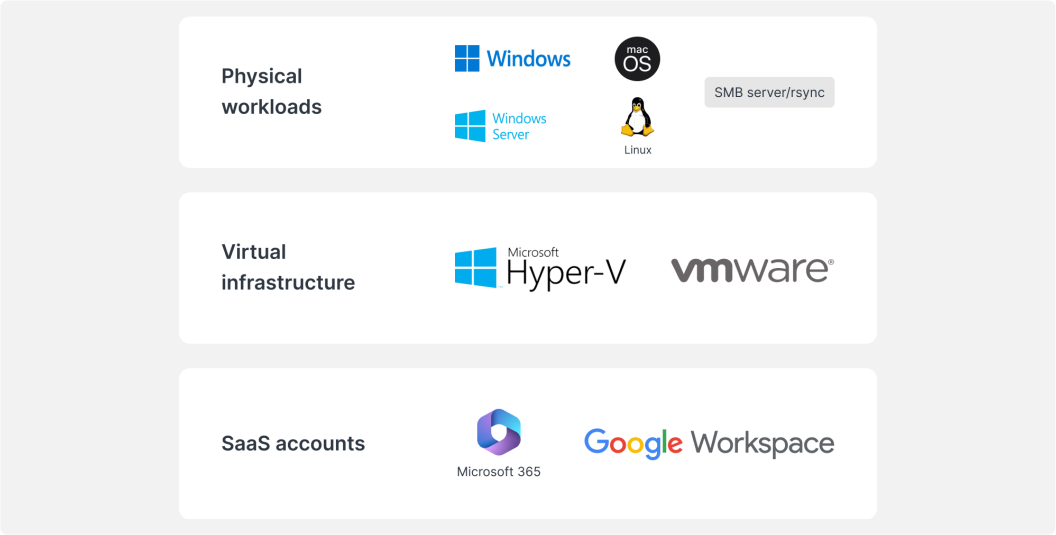
Pomocí komplexního úplného zálohování systému a flexibilního obnovení na úrovni souborů dokážete ochránit koncové body v případě škodlivých útoků.

Virtuální infrastruktura

Zálohujte virtuální počítače se systémy VMware® vSphere™, Microsoft® Hyper-V® a jednotky LUN pomocí výkonných technologií snižujících objemy dat.

Účty SaaS

Povolte průběžnou ochranu dat uložených v cloudu s automatickou detekcí nově přidávaných účtů.



Efektivní obnovení

Rychlým obnovením záloh z místního nebo vzdáleného systému Synology dokážete minimalizovat výpadek důležitých produkčních systémů.

Téměř nulové hodnoty RTO

Připojením snímků záloh v systému VMware®, Hyper-V® nebo v aplikaci Synology Virtual Machine Manager dokážete obnovit práci nejrychlejším možným způsobem. Obnovením virtuálních počítačů do alternativního hypervisoru předejdete narušení služeb.

Minimální hodnota RPO

Nakonfigurujte frekvenci zálohování podle svých potřeb a minimalizujte množství dat, která by mohla být při útoku potenciálně zasažena. Technologie přírůstkového zálohování a deduplikace umožňuje rychle ochránit systémy.

Intuitivní použití

Umožněte zaměstnancům ještě před obnovením procházet a zobrazovat náhledy e-mailů, kontaktů a souborů v příjemném portálu, nabídněte uživatelsky přívětivější prostředí a snižujte zatížení týmů IT.

Přidání další vrstvy ochrany

Splňte požadavky strategie zálohování 3-2-1, ukládejte třetí sadu dat na jiném místě nebo do cloudu a ochraňte tak data před požárem, přírodní katastrofou nebo krádeží.

Do vzdálených serverů

Ukládáním záloh do serveru Synology v sekundárním umístění se můžete chránit před fyzickými haváriemi a replikací neměnných snímků můžete rozšířit ochranu před ransomwarem.

Do cloudu

Zálohujte do libovolného známého poskytovatele cloudu a zabezpečte svoje data před neoprávněným přístupem prostřednictvím šifrování AES-256 na straně klienta. https://c2.synology.com/storage/nas

Používá se s důvěrou v různých oborech

„Řešení Synology [...] nám umožnila snížit výdaje za hardware serverů [...] a navíc se usnadnilo zálohování infrastruktury i pracovních stanic, protokolování systému a správy souborů.“
https://www.synology.com/company/case_study/Investortools

„Díky službě Active Backup for Business jsou nyní všechny naše zálohy centralizované a dostupné 24 hodin denně, což nám pomáhá minimalizovat výpadky a plnit požadavky zákona FERPA.“
https://www.synology.com/company/case_study/University_of_Washington

„[...] Služba Active Backup for Business nabízí fantastické rychlosti zálohování a vynikající výsledky při odstraňování duplicitních dat – záloha dat serveru o velikosti 58 TB měla velikost pouhých 28 TB. [...]“
https://www.synology.com/company/case_study/SHISEIDO_Taiwan_ABB

„[...] Služba Active Backup for Business [...] umožňuje centralizovat a spravovat všechny úlohy zálohování z jediné konzole. Rychlé a spolehlivé obnovení navíc zajišťuje provoz bez výpadků.“
https://www.synology.com/company/case_study/UNESCO

Časté dotazy

Co je to ransomware?

Ransomware je typ malwaru, který oběti zašifruje soubory. Útočníci poté požadují výkupné, jehož zaplacením podmiňují obnovení přístupu k datům, a často hrozí, že v případě nezaplacení výkupného data trvale zničí. Útoky ransomwarem mohou být velice ničivé a mohou způsobit velké finanční ztráty jednotlivcům i organizacím. Před útoky ransomwarem můžete chránit sebe i svoje zařízení aktualizováním softwaru a pravidelným zálohováním souborů.

Jaké typy ransomwaru existují?

Existuje mnoho různých typů ransomwaru a neustále probíhá vývoj nových variant. Mezi nejčastější typy ransomwaru patří:

- **Šifrovací ransomware** – Nejběžnější typ ransomwaru zašifruje soubory oběti tak, že přístup k těmto souborům nelze obnovit bez dešifrovacího klíče. Útočníci poté požadují výkupné za tento klíč
- **Locker ransomware** – Tento typ ransomwaru změní přihlašovací údaje počítače nebo zobrazí zprávu, která oběti zabrání v přístupu do systému. Útočníci poté požadují zaplacení výkupného za odemknutí počítače
- **Ransomware-as-a-Service (RaaS)** – Obchodní model, v rámci kterého útočníci nabízejí ransomware jiným jednotlivcům nebo skupinám, které poté provádějí samotné útoky. Ti první obvykle zajistí ransomware a zpracování plateb a ti druzí dostanou určité procento ze zaplaceného výkupného
- **Scareware** – Ransomware, který si klade za cíl oběti vystrašit a přinutit tak k zaplacení výkupného. Obvykle se toho snaží dosáhnout zobrazením falešných bezpečnostních výstrah nebo zpráv, které tvrdí, že počítač oběti je nakažen virem. Útočník poté požaduje zaplacení výkupného s tím, že následně domnělou infekci odstraní

Jakým způsobem se ransomware šíří?

Ransomware se obvykle šíří prostřednictvím phishingových e-mailů nebo zneužitím bezpečnostních děr v systému počítače. V rámci phishingového útoku útočník rozešle e-maily, které vypadají, jako by byly odeslány z oficiálního zdroje, například z banky nebo známé společnosti. Tento e-mail často obsahuje odkaz nebo přílohu a pokud na ně oběť klikne, nainstaluje se do jejího počítače ransomware. Zneužití bezpečnostních děr v systému probíhá podobně, útočník ale využije chybu v zabezpečení systému a nainstaluje ransomware bez vědomí oběti. V obou případech platí, že po instalaci se ransomware dokáže rychle šířit do dalších počítačů ve stejné síti.

Jakým způsobem probíhá typický útok ransomwarem?

Typický útok ransomwarem probíhá takto:

1. Útočník získá přístup k počítači oběti, buď odesláním phishingového e-mailu nebo zneužitím bezpečnostních děr v systému
2. Jakmile má útočník přístup k počítači oběti, nainstaluje do systému ransomware
3. Ransomware zašifruje soubory oběti a uživatelé k nim tak ztratí přístup
4. Útočník poté požaduje od oběti výkupné, obvykle ve formě digitální měny, například bitcoinů, výměnou za dešifrovací klíč, kterým by bylo možné zašifrované soubory odemknout
5. Pokud oběť výkupné zaplatí, útočník poskytne dešifrovací klíč a oběť získá ke svým souborům opět přístup. Neexistuje ale žádná záruka, že útočník klíč poskytne, navíc i v případě, že ho poskytne, mohou být soubory oběti v důsledku procesu zašifrování zničené nebo poškozené

Je důležité si uvědomit, že existuje mnoho variant tohoto procesu a ne všechny útoky ransomwarem probíhají přesně tímto způsobem. Některé útoky nemusejí vůbec zahrnovat zašifrování souborů a při jiných může docházet k jiným způsobům vydírání.

Jak se můžu ransomwarem nakazit?

Ransomwarem se můžete nakazit několika způsoby. Jedním z nejčastějších způsobů je kliknutí na škodlivý odkaz nebo přílohu ve phishingovém e-mailu. Tento typ e-mailu je navržen tak, aby vypadal věrohodně, často vypadá jako od známé společnosti nebo organizace. Když kliknete na odkaz nebo přílohu, nainstaluje se do vašeho počítače ransomware. Dalším způsobem, jak se můžete ransomwarem nakazit, je navštívit napadenou webovou stránku. Tyto webové stránky byly napadeny útočníky, kteří do nich vložili kód, který automaticky nainstaluje ransomware do počítače, ze kterého takovou webovou stránku navštívíte. Ransomwarem se můžete také nakazit stažením infikovaných souborů z internetu. Může k tomu dojít například tak, že stáhnete soubor z podezřelých webových stránek nebo soubor, který sdílel někdo, koho neznáte. Stručně řečeno, při procházení internetu je důležité být opatrný a neklikat na odkazy ani nestahovat soubory z neznámých zdrojů. Můžete se tak ochránit před nákazou ransomwarem a dalšími typy malwaru.

Kdo bývá cílem ransomwaru?

Útoky ransomwarem se mohou zaměřit na kohokoliv, kdo používá počítač nebo jiné zařízení připojené k internetu. Pravděpodobnost napadení se ale u různých skupin uživatelů liší. Útoky ransomwarem se proto častěji zaměřují na firmy, které mají cenná data a mohou být ochotnější zaplatit výkupné za jejich obnovení. Častými cíli jsou také nemocnice, školy a další organizace poskytující důležité služby, protože útok ransomwarem může narušit jejich provoz a ohrozit životy lidí. Útoky ransomwarem se ale mohou zaměřit také na jednotlivce. V takových případech se útočníci mohou pokusit získat peníze od oběti hrozbami, že v případě nezaplacení výkupného odstraní jejich soukromé soubory nebo zveřejní citlivé informace. Cíle útoků ransomwarem se často vybírají podle hodnoty jejich dat a ochoty zaplatit výkupné za jejich získání zpět.

Jaká rizika jsou spojena se zaplacením ransomwaru?

Zaplacení výkupného útočníkovi ransomwarem může vypadat jako nejsnadnější způsob získání svých souboru zpět, ale ve skutečnosti se může jednat o velice riskantní rozhodnutí. Se zaplacením výkupného je spojeno několik rizik, například:

- Neexistuje žádná záruka, že útočník dešifrovací klíč skutečně poskytne. V mnoha případech oběti, které výkupné zaplatí, klíč nikdy neobdrží a ke svým souborům přístup nezískají
- Zaplacení výkupného může motivovat útočníky k dalším útokům. Pokud útočníci vědí, že oběti jsou ochotné výkupné platit, zvyšuje se pravděpodobnost, že v budoucnu provedou další útoky
- Po zaplacení výkupného se tak můžete stát cílem budoucích útoků. Pokud útočník ví, že jste ochotni výkupné zaplatit, může se zvýšit pravděpodobnost, že budete v budoucnu cílem dalšího útoku
- Zaplacení výkupného může být v rozporu se zákonem. V některých případech může být zaplacení výkupného kriminální organizaci považováno za financování terorismu nebo jiných nezákonných aktivit

Takže zatímco se zaplacení výkupného může jevit jako nejsnadnější způsob obnovení souborů, ve skutečnosti se může jednat o velice riskantní rozhodnutí. Před rozhodnutím je důležité pečlivě zvážit rizika.

Jaká bývá cena ransomwaru?

Náklady spojené s útokem ransomwarem se mohou významně lišit na základě celé řady faktorů, například typu použitého ransomwaru, počtu zašifrovaných souborů a efektivity útoku. V některých případech mohou být náklady spojené s útokem ransomwarem relativně nízké a útočníci mohou požadovat výkupné ve výši několika stovek dolarů. V jiných případech mohou být tyto náklady mnohem vyšší a útočníci mohou za obnovení přístupu k souborům oběti požadovat tisíce dolarů nebo i více. Kromě přímých nákladů spojených se zaplacením výkupného mohou útoky ransomwarem zahrnovat ještě významné nepřímé náklady. Útok ransomwarem může například způsobit odstávku a ztrátu produktivity, které následně způsobí ztrátu zisku a příjmů. Může také dojít k poškození pověsti společnosti a důvěry zákazníků a k následným negativním dopadům na celou firmu. Tyto nepřímé náklady jsou často mnohem vyšší než samotné výkupné.

Jaké bývají příznaky ransomwaru?

Příznaky útoku ransomwarem se liší podle konkrétního typu použitého ransomwaru. Mezi běžné příznaky ale patří:

- Vaše soubory jsou zašifrované a vy k nim nemáte přístup
- Obdržíte zprávu od útočníka s žádostí o zaplacení výkupného výměnou za dešifrovací klíč
- Vidíte, že jsou ve vašem počítači spuštěné neznámé programy nebo procesy
- Váš počítač se zpomalí nebo přestane reagovat
- Váš počítač začne zobrazovat neobvyklé chybové zprávy nebo místní okna

Pokud nabudete podezření, že je váš počítač infikován ransomwarem, je důležité jednat rychle. Odpojte počítač od internetu, aby nedocházelo k dalšímu šíření ransomwaru.

Jak lze předcházet útokům ransomwarem?

Útokům ransomwarem můžete předcházet několika způsoby, například:

- Používejte prověřený antivirový nebo jiný bezpečnostní software a zajistěte, aby byl vždy aktuální. Můžete tak ochránit svůj počítač před ransomwarem a jinými typy malwaru
- Buďte opatrní při otevírání příloh e-mailů nebo odkazů v e-mailech. Ransomware je často doručován prostřednictvím phishingových e-mailů, takže je důležité dávat pozor, na co klikáte
- Pravidelně aktualizujte svůj operační systém a další software. Aktualizace softwaru často zahrnují bezpečnostní opravy, které pomáhají chránit počítač před ransomwarem a dalšími hrozbami
- Pravidelně zálohujte svoje soubory. Pomůžete tak svoje data ochránit v případě, že by byl váš počítač infikovaný ransomwarem. Dodržujte zásady některé z doporučených strategií zálohování, například strategie zálohování 3-2-1
- Uvědomte si rizika spojená s ransomwarem a informujte o těchto hrozbách ostatní osoby ve své organizaci. Pomůžete tak předcházet útokům ransomwarem a usnadníte zjištění případné infekce a reakci na ní

Nejlepším způsobem předcházení útokům ransomwarem je dávat si pozor a podniknout kroky k ochraně svého počítače a dat. Snížíte tak riziko útoku ransomwarem a usnadníte obnovení v případě, že k takovému útoku dojde.

Jakým způsobem mě může ochránit před ransomwarem Synology?

Nejdůležitějším prvkem ochrany před útokem ransomwarem je prevence. Kromě svého antivirového softwaru používejte ještě tato řešení Synology:

- **Zabránění přístupu** – Rozšíření ransomwaru můžete omezit nastavením oprávnění pro soubory, aplikace i přístup a konfigurací zabezpečených přihlašovacích údajů pomocí služeb Secure SignIn a C2 Password
- **Ochrana zařízení** – Zastaralé systémy jsou ohroženější. Aktualizujte všechna svoje zařízení NAS najednou pomocí systému centralizované správy (CMS) Synology a chraňte ostatní zařízení pomocí skupinových zásad ve službách Synology Directory Server a C2 Identity
- **Dávejte si pozor na podezřelé soubory** – Běžným způsobem šíření ransomwaru je nevyžádaná pošta a phishingové e-maily obsahující podezřelé soubory. Služba Synology MailPlus nabízí účinnou ochranu před malwarem a nevyžádanou poštou
- **Kontrola zranitelností** – Služba Synology Security Advisor zajišťuje průběžné vyhledávání malwaru, zranitelností a neobvyklých aktivit při přihlašování. Implementací doporučených změn zvýšíte zabezpečení svého zařízení NAS.
  https://www.synology.com/dsm/overview/security

Další způsoby ochrany dat

Správa všech zařízení

Rozsáhlá nabídka funkcí umožňuje centrálně spravovat oprávnění pro přístup k datům, stav softwaru, stav systému a další.
https://www.synology.com/dsm/overview/administration

Monitorování všech systémů

Zjišťování podezřelých aktivit přihlášení, správa aktualizací a monitorování stavu zařízení bez ohledu na to, kde se vaše zařízení nacházejí.
https://www.synology.com/dsm/feature/active-insight

Ochrana dat

Dodržujte zásady pravidla zálohování 3-2-1, které vám pomohou ochránit data před neúmyslnou či úmyslně škodlivou změnou nebo odstraněním.
https://www.synology.com/dsm/solution/data_backup

Ochrana ze všech možných perspektiv

Stáhněte si náš kontrolní seznam kybernetické bezpečnosti a zjistěte svá slabá místa pro případ útoku hackerů.
https://global.download.synology.com/download/Document/Software/Brochure/Firmware/DSM/7.0/csy/Se

Jak začít

Obraťte se na nás

Další informace vám poskytne regionální prodejní oddělení
https://www.synology.com/form/inquiry/sales

Kde nakupovat

Najděte partnera Synology ve vašem regionu
https://www.synology.com/wheretobuy

Notes:

1. eSentire, 2022 Official Cybercrime Report (Oficiální zpráva o kybernetické zločinnosti 2022) https://www.esentire.com/resources/library/2022-official-cybercrime-report

Ochrana organizace před ransomwarem

https://www.synology.com/cs-cz/dsm/solution/ransomware

Synology webová stránka

https://www.synology.com/

Obraťte se na nás

https://www.synology.com/company/contact_us