OCHRANA PROTI RANSOMWARU

Obecně lze ochranu proti ransomwaru rozdělit na procesní a technická opatření. Mezi procesní opatření lze zařadit pravidelná školení zaměstnanců, pravidelné nastavení kontrol aktualizace a zálohování dat nebo proces schvalování výjimek pravidel na firewallech. K technickým opatřením patří správná konfigurace zařízení v síti, sandboxing, pravidelné patchování operačních systémů nebo oprava zranitelností aplikací.

STRATEGIE OCHRANY

V této kapitole jsou popsány postupy ochrany proti malware a charakteristika základních bezpečnostních prvků ICT infrastruktury, které jsou obecně platné při návrhu strategie ochrany kybernetické bezpečnosti.[1]

METODIKA OCHRANY

Bezpečnostní strategie by měla být založena na dvou obecných principech:

- pre-infection - minimalizace rizika, že k nákaze dojde
  Vzhledem k vysoké stupni závislosti moderních organizací na ICT technologiích a infrastruktuře je nezbytně nutné již v návrhu procesních i technických opatření uvažovat o snížení rizika úspěšnosti útoku.
  Tato oblast by měla zahrnovat dvě fáze ochrany:
  - Predikce
  - Prevence
- post-infection - minimalizace negativních dopadů úspěšného útoku
  Je třeba si uvědomit, že přes úspěšnou implementaci všech navržených technických i procesních opatření, existují rizika, která nelze zcela eliminovat. Proto je vhodné zavést postupy a opatření pro co nejrychlejší detekci infekce, její rychlé zastavení a zotavení z útoku.
  Tato oblast by měla zahrnovat následující dvě fáze ochrany:
  - Detekce
  - Reakce a obnova

ČTYŘI FÁZE OCHRANY

Při současné komplexitě ICT systémů se nelze plně spolehnout na jeden způsob ochrany, např. běžná technická řešení založená především na detekci pomocí signatur. Pro moderní organizaci je nezbytné přijmout celkovou koncepci strategie ochrany.

Tato bezpečnostní strategie by měla zahrnovat optimálně 4 fáze:

- Predikce
- Prevence
- Detekce
- Reakce a obnova

---

[1] Web SANS, https://www.sans.org/reading-room/whitepapers/malicious/enterprise-survival-guide-ransomware-attacks-36962

Následující podkapitoly podrobněji rozvádějí jednotlivé fáze a uvádějí mimo jiné výčet předpokladů, které jsou v dané fázi kritické pro úspěšnou implementaci strategie jako celku.

PREDIKCE

Tato fáze slouží k identifikaci klíčových prvků infrastruktury, kriticky důležitých systémů a datových úložišť. Zároveň umožňuje průběžně hodnotit stav a úroveň zabezpečení těchto prvků.

Provedení této přípravné fáze strategie ochrany by měla poskytnout odpovědi na základní otázky:

- Které systémy jsou zranitelné, a které ze zranitelností jsou nejkritičtější?
- Které ze zranitelných systémů jsou kriticky důležité pro chod organizace?
- Která data mají z pohledu útočníka největší hodnotu a která jsou nejdůležitější pro organizaci, nebo např. pro zákazníky (viz např. oblast ochrany osobních údajů – GDPR)?
- Kdo opravdu potřebuje které přístupy, data a funkce k výkonu své práce?
- Jaké je povědomí zaměstnanců o hodnotě dat se kterými pracují, a o různých formách útoků?
- Umí zaměstnanci rozpoznat hrozbu, jestliže jí čelí?
- Jsou administrátoři bezpečnostních prvků proškoleni na včasnou reakci a jsou schopni rychlé reakce na incident?

Zodpovězením těchto otázek však proces sběru informací, inventarizace a vyhodnocování nesmí skončit. Neustále jsou v nových i starších verzích systémů objevovány zranitelnosti, kontinuálně probíhá vývoj technologií i technik útoku. Je proto třeba zavést periodický proces vyhodnocování rizik a na něj navazující proces jejich řešení.

PREVENCE

Preventivní fáze je složena z opatření technického charakteru a opatření procesního charakteru, velmi důležité je vnímat a hodnotit jednotlivé kroky v kontextu celkové strategie. A snížit tak riziko kritického selhání vytvořené nedostatečnou implementací některého z prvků bezpečnostní strategie. Preventivní fáze navazuje na fázi Predikce.

Výstupy zjištění identifikace rizik a předvídání, která data jsou z hlediska útočníka a organizace zajímavá, lze následně preventivně minimalizovat, např.:

- Přístupy uživatelů k serverům, k datům atd.
- Přístupy uživatelů k externím zdrojům (Internet)
- Riziko úspěšné exploitace zranitelnosti různých zařízení
-

Je nutné pravidelně kontrolovat zranitelnosti všech ICT prvků, a pokud možno ty kritické co nejrychleji odstraňovat, nebo alespoň kontrolovat doplňkovými opatřeními. Toto doporučení mimochodem patří mezi absolutní základy kybernetické hygieny, které je však bohužel mezi těmi nejčastěji nedodržovanými.

Na základě zjištění znalostí a povědomí zaměstnanců o metodách útočníků a technikách provedení útoků lze navrhnout:

- Školení uživatelů, včetně pravidelných testů „na živo“ – například zasílání falešných zpráv, aby si zaměstnanci zvykli je rozlišovat
- Školení zaměstnanců IT a zejména bezpečnostních specialistů

- Vytvoření trvalého týmu CIRT (Cyber Incident Response Team) z bezpečnostních pracovníků a administrátorů nebo navrhnout částečný outsourcing CIRT

Realizace této fáze může být částečně splněna implementací běžných bezpečnostních technologií. Technologie založené na detekci pomocí známých signatur, jsou však pouze reaktivním opatřením, které má logicky vždy určité zpoždění oproti útočníkům. Nelze se tedy spoléhat jen a pouze na ně, je na místě zvážit investici do pokročilejších metod ochrany.[2]

Z technických opatření minimalizují rizika především instalace antivirů, firewallů, IPS a sandboxů, jakož i update informačních systémů na základě priorit určených ve fázi Identifikace a predikce, tedy:

- Blokace přístupů, které nejsou nezbytně nutné pro výkon pracovní činnosti
- Blokace aplikací, které nejsou nezbytně nutné
- White listing nezbytně nutných aplikací
- Není-li zavedena, pak instalace pokročilé emailové ochrany - Anti-spam a Anti-phishing

Doporučujeme implementovat některá z řešení pro detekci a blokaci škodlivého kódu, a to optimálně na několika vrstvách zároveň, a několika technologiemi:

- na externím perimetru (komunikace s Internetem), zejména na emailové a webové komunikaci
- na interních perimetrech (v interně segmentované síti)
- na koncových stanicích

Z hlediska technologií doporučujeme kombinaci:

- nástroje pro detekci a blokaci podezřelých komunikací a souborů (firewally, IPS a sandboxy)
- nástroje pro detekci anomálií v interním provozu

Sandbox je prostředí, které co nejvěrněji simuluje chování uživatelské stanice, včetně chování uživatele. Tato metoda vede k poměrně spolehlivé detekci (a následně blokaci) škodlivého kódu obecně včetně ransomware. Při využití sandboxingu je vhodné ověřit spolehlivost dané technologie, protože moderní malware již dokáže sandboxingovou technologii detekovat na základě vlastních signatur.

Vzhledem k novým vývojovým trendům je vhodné, aby zvolené řešení umožňovalo sanitaci dokumentů, před jejich stažením nebo otevřením, tzn. očištění dokumentů od maker a hypertextových odkazů.[3][4]

---

[2]TrendMicro,http://www.trendmicro.com/cloudcontent/us/images/ransomware/sb01_smb_ransomware_160518us.pdf

[3] Web Symantec, https://www.symantec.com/connect/articles/hardening-your-environment-against-ransomware

[4] Web Kaspersky, A practical guide to cryptor attacks, http://media.kaspersky.com/pdf/guard-against-crypto-ransomware-kaspersky-guide.pdf

DETEKCE

V této fázi je možné spolehnout se na detekci pomocí vyhodnocování hlášení antivirových systémů. Tato metoda však nepostihne útok v jeho šíři, často je např. ignorována souvislost scanování sítě ze strany útočníka a následujícího útoku.

Pro detekci útoku může být velmi výraznou výhodou implementace SIEM, nebo alespoň centrální správy a analytických činností systémových hlášení z prvků a aplikací ICT infrastruktury. Vzhledem k nárůstu počtu spravovaných zařízení a jejich složitosti je potřeba uplatnit nástroje pro včasnou detekci anomálií. Tento postup vede nejen k včasné detekci problému a jeho odstranění, ale též k pružnější reakci na vzniklý incident.

Mezi moderní detekční metody patří detekce anomálií chování, která umožňuje snáze detekovat činnost útočníků. Běžným jevem je např. scanování zařízení v síti, které předchází útoku. Anomálie v DNS provozu (např. použití jiných než schválených DNS serverů, nebo vyšší než očekávaný DNS provoz) mohou indikovat MITM útok případně špatné nastavení DNS serveru, nebo pokus uživatele použít neschválený DNS server. Pro detekci a včasnou analýzu anomálií je nutné využít maximum oblastí (vrstev), ke kterým patří zejména endpointy (nejen klasické PC, ale i mobilní platformy), servery, sítě, aplikace (zejména email, web, …) a chování uživatelů.

Mezi běžné detekční metody dnes patří také využití honeypotů, které je nutné udržovat v aktualizovaném stavu. Proto je vhodné zvážit outsourcing jejich správy, jestliže tato aktivita nepatří mezi hlavní činnosti ICT provozního týmu organizace.

Pro detekci infekce je vhodné sledovat anomálie ve všech možných oblastech, např.:

- Chování uživatelů
- Chování koncových stanic
- Servery
- Segmenty sítě

Uživatelé

Je třeba sledovat anomální chování ze strany uživatelů např. mnohanásobná selhání přihlášení v krátkém časovém intervalu, pokusy o autentizaci pomocí pass the hash metody atp. Napadený uživatelský účet je třeba zablokovat, toto opatření je možné též zahrnout v preventivní fázi, kde je na místě zvážit využívání sdílených uživatelských účtů zejména se zvýšenými privilegii.[5]

Koncové stanice

Anomálním chováním koncových stanic je např. výrazně zvýšený počet odesílaných e-mailových zpráv obsahujících totožný nebo obdobný dokument, případně IP Spoofing, odesílání DNS packetů typických pro servery apod. Stanici vykazující anomální chování je třeba izolovat.

Servery

Anomálním chováním serveru je např. komunikace nešifrovaným Telnet se zahraniční zdrojovou IP, úspěšný příchozí SSH požadavek ze vzdálené zahraniční IP, výpadek služby a její následné naskočení etc.

[5] Web TrendMIcro, https://www.trendmicro.com/cloud-content/us/pdfs/trend_micro_ransomware_defense.pdf

Segmenty sítě

Vysoký provoz ICMP, TCP scany apod. mohou být indikátorem šíření malware, je proto nutné monitorovat provoz na chráněné síti a pro jednotlivé segmenty. Zároveň je třeba mít k dispozici nástroj, který umožní infikovaný segment izolovat a provést opravné kroky.

V případě ransomware specificky, půjde u detekce anomálií např. o uzamčení privilegovaných uživatelských účtů. U koncových stanic o uzamčení systémových disků, případně zašifrování datového úložiště. Obdobně u serverů nebo výpadku služeb bude předcházet scan a následné zašifrování systémového disku nebo datového úložiště, což může vyvolat selhání dalších služeb např. nemožnost přihlásit se k Active directory, nemožnost pracovat s daty v databázi.[6]

REAKCE A OBNOVA

Tato fáze strategie ochrany je reakcí na incidenty a jevy zjištěné v předcházejících fázích a nabízí prostor pro realizaci protiopatření. Jednotlivá protiopatření se obecně dělí do několika oblastí:

Plánování reakce

Protiopatření v oblasti plánování zajišťují úspěšné zavedení bezpečnostní strategie do praxe. Mezi klíčová protiopatření v této oblasti patří:

- **Disaster Recovery plány**

Tvorba a implementace těchto plánů umožňují včasné zotavení základních funkcí sítě po úspěšném útoku. Je-li plán správně implementován, pomáhá částečně ochránit kriticky důležité systémy.[7]

- **Incident Recovery plány,**

K incidentům bezpečnostního charakteru dochází velmi často a některé předběžné jevy a jevy dříve považované za incident se staly naprosto běžnou součástí každodenního provozu na síti. Za incident je dnes třeba považovat např. selhání systému v důsledku DDoS útoku, úspěšný phishing a izolaci napadené stanice, nebo prosté selhání systému v důsledku nevhodné konfigurace.[8]

- **Testování scénářů v praxi**

Testování scénářů slouží k praktickému ověření bezpečnostní strategie jako celku pomocí simulovaného útoku, který svými charakteristikami odpovídá posledním trendům v této oblasti.

---

[6]Christopher M. Frenz a Christian Diaz, Anti-Ransomware Guide, Web OWASP, https://www.owasp.org/images/a/a8/Anti-RansomwareGuide.pdf

[7] Web Infrascale, https://www.infrascale.com/wp-content/uploads/pdf/Infrascale-Top-Six-Ransomware-Defense-Strategies.pdf

[8] Web Customtech, http://www.customtech.com/assets/Ten-Tips-Ransomware-002.pdf

Karanténa

Pod tímto pojmem se rozumí schopnost rychlého omezení dalšího šíření malware. Karanténa a možnost jejího rychlého nasazení není již záležitostí čistě jen infikovaných souborů, jestliže jsou detekovány anomálie v síti je třeba zdroj těchto anomálií izolovat a provést následná opatření.

Obnovení činnosti

Po úspěšném útoku, je nutné v krátkém čase shromáždit podklady pro forenzní šetření a zároveň co nejrychleji obnovit běžný provoz sítě. K tomu slouží předem vytvořené zálohy a CIRT tým.

Inteligentní zálohování

Off-line zálohy slouží k obnovení činnosti, kdy není možné použít online zálohy, neboť došlo k jejich zašifrování a je za jejich zpřístupnění požadován poplatek. V případě neexistence off-line záloh a absenci postupu pro obnovení dat v důsledku slabiny použitého ransomware, je obvykle nutné zaplatit požadovanou sumu útočníkovi.

Segmentace záloh spočívá v odmítnutí přístupu jedné uživatelské role ke zbytečně „širokému“ množství záloh.

Není obvykle možné zálohovat všechna data a není možné veškerá data uchovávat. Proto je nutné zvolit různé stupně ochrany dat jejich zálohováním v různých úložištích.

Schopnosti obnovy

Pro testování této fáze obnovy je rozhodujícím faktorem dostupnost záloh, dostupnost náhradního HW. Omezujícím faktorem pak může být nutnost shromáždění dat pro forenzní šetření, což může výrazně prodloužit dobu zásahu. K minimalizaci nákladů a ztrát je proto vhodné nejen proškolit zaměstnance, ale pravidelně provádět trénink a vyhodnocovat jeho časový průběh.

Forenzní šetření

Je obvykle mimo technické znalosti běžných administrátorů a je nezbytné vyčkat příjezdu forenzního technika, který je zároveň soudním znalcem v tomto oboru. Pokud není forenzní expert zároveň soudně uznávaným znalcem, nebude možné shromážděná data použít v trestním řízení.

Obecně lze konstatovat, že takový postup není vždy žádoucím a vhodným, značné množství útoků je prováděno útočníky v jurisdikcích, jejichž spolupráce pokud vůbec existuje, je pomalá. Případně může kriticky významný důkaz elektronického charakteru např. navázání spojení na VPN server podlehnout zkáze dříve, než proběhne forenzní šetření (bullet proof hosting, bullet proof VPN etc.)

Schopnost detailní analýzy

Je obvykle předmětem outsourcingu, nelze po každém technikovi požadovat reverzní inženýrství v oblasti šifrovaného malware. Je však vhodné seznámit technický personál i běžné uživatele s běžnými postupy, které zajistí hladký průběh této fáze a urychlí fázi obnovení funkcí.[9]

[9] Web Symantec, https://www.symantec.com/connect/articles/hardening-your-environment-against-ransomware