PREVENCE RANSOMWARE A JINÝCH HROZEB
DOPORUČENÉ POSTUPY

KONFIGURACE E-MAIL OCHRANY

- Blokovat spustitelný obsah *(exe, js, vba, atd.)* a to i pokud je obsažen v archivech *(např. exe v zip)* nebo dokumentech *(vba, makro v doc)*.
    - pro zasílání takového obsahu používat pouze k tomu určený kanál, obsahující kontroly obsahu a audit logy *(např. SOFiE)*, ostatní blokovat *(Dropbox, Ulož.to, Úschovna.cz)*
- Blokovat šifrované soubory, což jsou často archivy a Office dokumenty. *(jejich obsah nelze zkontrolovat a může být nebezpečný)*.
- E-mail gateway doplnit o sandboxing e-mailových příloh a URL *(např. FortiSandbox)*.
- Implementovat standard DMARC *(s politikou reject)*. Optimálně využít standard DNSSEC.
- Používat kvalitní e-mail gateway s aktualizovaným komerčním antivirem a antispamem.
- Nepoužívat sekundární a další MX záznamy obcházející primární gateway s bezpečnostními kontrolami.
- Příchozí SMTP spojení na e-mail server/platformu (*např. Office365 nebo G Suite)* povolit pouze z e-mail gatewaye, aby nebylo možné gateway obejít a doručovat e-maily přímo.
- Blokovat přílohy s neobvyklými archivy *(pokud možno povolit pouze .zip)*. Mohou obsahovat malware a mohou obejít kontrolu některými bezpečnostními nástroji.

OCHRANA NA PERIMETRU A LAN

- Vhodná segmentace sítě *(např. pomocí VLAN)* na co nejmenší vhodné celky a segmentační firewall pro filtrování komunikace mezi těmito segmenty *(VLANy)*. Povolit jen nutnou komunikaci, ostatní zakázat *(nikoliv obráceně)*.
- S tím související důsledné využívání demilitarizovaných zón *(DMZ)* pro vše přístupné přímo z Internetu. Z DMZ by také neměl být možný přístup dále do LAN, pouze obráceně *(z LAN do DMZ)*.
- Pro přístup zvenku používat vždy VPN. Nemapovat porty z Internetu do vnitřní sítě. Pokud to nějaká služba vyžaduje, měla by být v DMZ.
- Používat aktuální dobře nakonfigurovaný firewall s moderními funkcemi *(IPS/IDS, webfiltr, aplikační filtr, antivir)*.
- Používat izolaci klientů. Běžná funkce u lepších WiFi, ale vhodné ji nasadit i pro switche, tj. stanice “na kabelu”, pokud to switche podporují. *(aby nedocházelo k šíření škodlivého kódu mezi stanicemi přes lokální zranitelnosti)*
- Blokovat komunikaci se známými botnety a jejich C&C servery *(funkce NGFW firewallů)*.
- Implementace honeypotu spolupracujícího s firewallem na blokaci zjištěných útoků.
- Využívat doplňkové seznamy s IP adresami pro blokování závadových komunikací. Doporučujeme využít např. z NIC.CZ *(zdarma)*
- Provádět inspekce HTTPS a jiného SSL provozu.
- Blokovat komunikaci se sítěmi typu TOR.
- Provádět detailní síťový monitoring celé sítě.
- Blokovat přístup do sociálních sítí, úložišť typu Dropbox a jiných.

Zahrnuje doporučení NÚKIB

KONFIGURACE STANIC A SERVERŮ WINDOWS

- Nepoužívat administrátorské ani jinak privilegované účty pro běžné uživatele a běžnou práci.
- Neukládat data lokálně na stanice.
- Centrální instalace bezpečnostních záplat a aktualizací *(Patch management)* všech používaných produktů/ software na stanicích.
  - Mimo MS/WSUS řešit také aktualizace Acrobat Reader, Java atp.
- Pravidelná aktualizace serverů.
- Používat aktualizovaný antivirový systém.
- Pomocí doménových politik *(GPO)*:
  - Zakázat makra pro Microsoft Office.
  - Volitelně v MS Office povolit pouze bezpečné limitované funkce.
  - Zakázat používání vlastních USB disků a jiných externích datových nosičů.
- Pro Internet využívat jen bezpečné aktuální prohlížeče.
  - Pokud je nutné používat zastaralý a nebezpečný IE, pak jedině na interní izolované aplikace.
- Omezení pro vzdálenou správu:
  - RDP zakázat nebo povolit pouze z VLANy IT administrátorů.
  - TeamViewer spouštět jen na vyžádání IT a potom opět vypínat.
- Používat menší množství stejných typů HW i SW konfigurací stanic. Mít pro tyto připravený postup rychlé automatické *(re)*instalace *(referenční čistý image)*.
- Minimalizovat přístup vlastních zařízení uživatelů *(BYOD)* do sítě, např. povolit pouze do dedikované VLANy.
- Pro přístupy administrátorů používat vedle hesel také MFA ověření, kdekoli je to možné.
- MS servery s Active directory provozovat ve vlastní VLAN. Pro nejvyšší bezpečnost servery nemusí mít přímý přístup na internet a aktualizovat je lze přes WSUS.

BACKUP MANAGEMENT

- Pravidelná kontrola zálohování včetně ověření funkčnosti záloh.
- Více verzí záloh v čase zpětně, nikoli jen poslední aktuální kopii dat. Např. schéma: týden zpět denní zálohy, měsíc zpět týdenní zálohy, tři měsíce zpět měsíční zálohy.
- Minimálně dvoustupňové zálohování, tj. musí existovat i sekundární kopie/záloha záloh. Nejlépe offsite *(v cloudu, jiné lokalitě, atd.)*. Sekundární zálohy nesmí být přímo přístupné *(např. nesmí být jen jiný síťový disk)*. Pro zvlášť citlivé provozy/data musí existovat i offline zálohy *(např. pásky v trezoru)*.
- Tzv. pravidlo 3-2-1 pro zálohování říká, že mají existovat minimálně tři kopie dat na minimálně dvou různých médiích a minimálně jedna v jiné lokalitě.
- Definovaná politika pro ukládání, zálohování a obnovu dat - kde jsou jaká data, např.:
  - stanice - žádná data - obnova *(re)*instalací referenčního image
  - servery
    - SQL - nutná je konzistentní záloha databáze k tomu určenými nástroji a postupy *(dump databáze)* - obnova = instalace nového prázdného serveru *(ideálně automaticky z image)* a natažení dat databáze ze zálohy DB
    - File server - verzování, kopie souborů, apod.
    - Virtuální servery - zálohy obvykle formou snapshotů celé VM pro rychlou obnovu
  - disková pole, NAS
  - cloudy a data v nich *(soubory, databáze, služby)*
- Zálohy by měly být šifrované, neboť obvykle obsahují citlivá data.

Příklad phishingového emailu s kompromitovanou přílohou .doc:

SPRÁVA A POLITIKY HESEL

- Obecně je nutné zajistit, aby nebyla používána slabá hesla bez dalšího faktoru. Zejména tam, kde je možné jejich vzdálené zneužití.
- Není možné nechávat nastaveny výchozí účty a hesla od výroby/instalace/resetu. A to ani na zařízeních jen ve vnitřní síti.
- Při své práci používat účty s co nejnižšími oprávněními pro danou činnost.
- Využívat unifikované MFA řešení všude, kde je to možné.

1. UŽIVATELÉ

- Po běžných uživatelích nelze rozumně požadovat, aby používali komplexní nezapamatovatelná hesla, pravidelně je měnili, nikam si je nepsali, používali do každé služby jiné heslo, atd. Dobré řešení musí být tedy takové, které i bez splnění takovýchto požadavků zajistí dobrou úroveň bezpečnosti.
- Maximálně využívat systém "Single Sign On" *(SSO)*, kde jediným uživatelským účtem *(např. v Active Directory)* se uživatel autentizuje do všech potřebných služeb. To má následující výhody:
  - lze použít lepší heslo, když uživateli stačí zapamatovat jedno
  - účet lze na jednom místě deaktivovat, změnit heslo, atd.
- Je-li to možné, doplnit použití hesla druhým faktorem *(MFA - aplikace v mobilu, čipová karta, Yubico atd.)*. Heslo pak může být jednodušší, neboť samo o sobě nestačí k autorizaci.
- Nevyžadovat pravidelné změny hesel. Jedná se o překonaný koncept, který vede k tomu, že hesla jsou pak slabší, systematicky odvoditelná, nebo zapisována uživateli na nevhodná místa *(papírky, nešifrované soubory, aj.)*.

2. IT PRACOVNÍCI

- Správci a IT specialisté musí obvykle používat velké množství účtů do různých služeb a zařízení, kde není rozumně možné je sjednotit pod jeden systém SSO. Některé účty je navíc často třeba sdílet mezi více lidmi. Aby tak byla zachována dobrá úroveň bezpečnosti, je třeba:
- Používat vhodný správce hesel *(např. BitWarden, LastPass, KeePass, atd.)*, díky kterému:
  - Každý účet může mít unikátní komplexní náhodně generované heslo.
  - Lze zakládat kontejnery pro sdílená hesla a přidělovat k nim oprávnění. Lze snadno změnit sdílené heslo, aniž by museli všichni, kdo ho používají, o tom být informováni.
  - Lze stanovit a kontrolovat či vyžadovat plnění různých politik pro práci s hesly *(síla, unikátnost, zda je kompromitované ve známém úniku hesel, apod.)*.
  - Hesla jsou uložena šifrovaně, bezpečně a na k tomu určeném místě.
  - Přístup k heslům lze zabezpečit kvalitním vícefaktorovým ověřením.
  - Hesla lze použít offline/zálohovat pro případ nefunkčnosti správce hesel.

3. EXTERNÍ DODAVATELÉ

- Pro externí dodavatele používat systémy pro správu privilegovaných účtů *(např. CyberArk)*.
- Pro přístup využívat specializované Jump servery *(SSH, RDP,..)*.
- Pro ověření využívat univerzální MFA řešení.

NAŠE SLUŽBY A ŘEŠENÍ

- Bezpečnostní audity, analýzy a konzultace
- Penetrační testy *(interní a externí)*
- Konfigurační audity
- Pravidelné kontroly *(health checky)*
- Expertní konzultace ochrany před ransomware
- Analýzy shody s ZoKB, ISO 27000 a GDPR
- Školení administátorů a uživatelů
- Řešení havarijních situací při kybernetických incidentech

Sonpo

SONPO, a.s. | Klapkova 546, 182 00, Praha 8
www.sonpo.cz | sales@sonpo.cz