Ministerstvo zdravotnictví České republiky
Palackého nám. č 4, 128 01 Praha 2, IČ: 00024341

Technická doporučení ke zvýšení zabezpečení infrastruktury informačních technologií organizací ve zdravotnictví proti kybernetickým útokům

Pořadí revize	Provedené dne	Zpracoval	Schválil
Verze 1.0	6.5.2020	Akční výbor KB MZ ČR	Ing. Martin Zeman

Sledování dokumentu

Rozdělovník

JMÉNO	ORGANIZACE	PŘEDÁNO (dne)	Č. VÝTISKU
www.nsez.cz			Ke stažení

Historie verzí dokumentu

Verze	Vypracoval	Předmět	Datum
1.0	MZ ČR / NCEZ	Dokument k užívání	6.5.2020

Obsah

Seznam zkratek a pojmů

Zkratka	Význam
Active Directory	Adresářové služby implementované společností Microsoft – soubor uživatelů, počítačů a dalších zařízení podléhajících společným pravidlům
Administrátorský účet	Účet s nejvyšším oprávněním, který umožňuje spravovat zařízení
Blacklist	Seznam zařízení, s kterými dané zařízení nekomunikuje
DKIM	*DomainKeys Identified Mail* – nástroj pro elektronické podepisování odcházejících emailů
DMARC	*Domain-based Message Authentication, Reporting and Conformance* – systém pro validaci emailových zpráv za účelem detekování falešných emailů
Domain Controller	Počítač, kde je centrálně udržován aktuální stav uživatelů, počítačů, tiskáren a dalších zařízení
DRP	*Disaster Recovery Plan* – plán obnovy provozu po havárii
Elearning	Vzdělávací proces za použití výpočetní techniky
Firewall	Zařízení sloužící k řízení a zabezpečení síťového provozu
Firmware	Základní program, zprostředkující komunikaci s hardware a umožňující start počítače
GOVCERT	*Computer Emergency Response Team* – vládní skupina profesionálů, která řeší kybernetické události
Group Policy	Sada předvoleb pro nastavení prostředí pro uživatele a počítače
ICT	*Information and Communication Technologies,* Informační a komunikační technologie
IP	*Internet Protocol* – běžně používaný komunikační protokol v počítačových sítích
LAPS	*Local Administrator Password Solution* – systém pro správu lokálních administrátorských účtů
Logování	Záznam o činnosti uživatele nebo zařízení
Malware	Škodlivý software - program určený k poškození nebo vniknutí do počítačového systému
MZČR	Ministerstvo zdravotnictví České republiky
NCEZ	Národní centrum elektronického zdravotnictví (odbor MZČR)
NCKB	Národní centrum kybernetické bezpečnosti
Neprivilegovaný účet	Běžný účet, který neumožňuje spravovat zařízení
NSEZ	Národní strategie elektronického zdravotnictví
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost

Zkratka	Význam
Offline záloha	Záloha dat, která není okamžitě přístupná
Operační systém	Základní programové vybavení počítače (zařízení)
Perimetr	Rozhraní počítačového zařízení, oddělující zabezpečený a nezabezpečený prostor.
Phishing	Podvodná technika k získávání citlivých údajů
Proxy server	Prostředník mezi uživatelem a cílovým zařízením, který zprostředkovává spojení
Release management	Řízený proces nasazování nebo uvolňování softwaru
RDP	*Remote Desktop Protocol* – protokol pro vzdálené připojení k jinému počítači
Sandbox	Bezpečnostní mechanismus pro oddělení běžících procesů
Segmentace	Logické oddělení počítačových sítí s definovanými pravidly vzájemné komunikace
Sender ID	Jednoznačná identifikace odesílatele
Spam	Nevyžádané sdělení šířené internetem
Spear-phishing	Podvodná technika k získávání citlivých údajů zaměřená na konkrétní osobu, oblast nebo organizaci
SPF	*Sender Policy Framework* – emailový validační systém, který ověřuje IP adresu odesílatele emailu
SSH	*Secure Shell* – zabezpečený komunikační protokol pro vzdálený přístup z příkazového řádku
SSL 2	*Secure Socket Layer* verze 2 – šifrovací protokol vydaný v roce 1995, od roku 2011 není považován za bezpečný
SSL 3	*Secure Socket Layer* verze 3 – šifrovací protokol vydaný v roce 1996, od roku 2015 není považován za bezpečný
TLS 1.0	*Transport Layer Security* verze 1 – šifrovací protokol vydaný v roce 1999, od roku 2020 není považován za bezpečný
TLS 1.1	*Transport Layer Security* verze 1.1 – šifrovací protokol vydaný v roce 2006, od roku 2020 není považován za bezpečný
TLS 1.2	*Transport Layer Security* verze 1.2 – šifrovací protokol vydaný v roce 2008, současně doporučovaný protokol
TLS 1.3	*Transport Layer Security* verze 1.3 – šifrovací protokol vydaný v roce 2018, současně doporučovaný protokol
ÚZIS	Ústav zdravotnických informací a statistiky ČR
VPN	*Virtual Private Network* – vzájemné zabezpečené propojení počítačů přes nedůvěryhodnou počítačovou síť

Tabulka 1 Seznam zkratek a pojmů

Úvod

Tento stručný soubor technických doporučení, jejichž smyslem je přispět k dosažení základní úrovně zabezpečení infrastruktury informačních technologií organizací ve zdravotnictví proti kybernetickým útokům, vznikl v reakci na setrvalý růst kybernetických hrozeb, směřujících na zdravotnické organizace. Zvláštní pozornost si přitom zaslouží tato doporučení v organizacích, které nepodléhají explicitně legislativě kybernetické bezpečnosti a existuje tedy vyšší riziko, že problematice kybernetické bezpečnosti nevěnovaly dosud patřičnou pozornost. Takové organizace se tak mohou stát snadným cílem kybernetických útoků. Dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů.

Dokument by měl být využíván souběžně s doporučeními Národního úřadu pro kybernetickou a informační bezpečnost, zejména s Doporučenými bezpečnostními opatřeními k varování ze dne 16. dubna 2020.

1 Technická doporučení

Pro zvýšení zabezpečení před hrozbami v oblasti kybernetické bezpečnosti Ministerstvo zdravotnictví doporučuje provést následující opatření:

1.1 Oblast ochrany vnějšího perimetru

- V současné době se ukazuje na mnoha příkladech kritická hrozba publikování RDP a SSH do vnější sítě. Důrazně doporučujeme tyto služby z vnější sítě nepoužívat.
- Zablokujte ostatní vzdálené přístupy do infrastruktury a zablokujte otevřené služby do veřejné sítě, vyjma těch nezbytně nutných (své veřejné IP rozsahy můžete zkontrolovat např. ve vyhledávači shodan.io a zjistit tak historicky otevřené/zapomenuté porty, či služby dostupné z veřejné sítě).
- Pokud je to možné používejte firewally nové generace.
- Blokujte škodlivé IP adresy a domény, vytvořte tzv. Blacklist. Aktualizujte Blacklist pokaždé, když NÚKIB nebo MZČR publikuje nové informace o škodlivých adresách, nebo když se o takových adresách dozvíte z dalších relevantních zdrojů.
- Zajistěte centralizované a časově synchronizované logování síťových událostí, nejlépe na server v jiném segmentu sítě.

1.2 Oblast vnitřní počítačové sítě

- Členěte síť na menší celky (segmentace) a striktně oddělujte uživatelská práva napříč segmenty.
- Po vytvoření jednotlivých segmentů sítě přesuňte všechna zařízení do nových segmentů a nastavte omezující pravidla komunikace mezi segmenty.
- Sledujte síťový provoz pomocí vybraných síťových prvků nebo rozmístěním dedikovaných síťových sond. Sledujte komunikaci mezi klienty a servery, komunikaci klientů do internetu, komunikaci mezi servery i provoz na perimetru sítě a identifikujte provozní a bezpečnostní problémy (např. neúměrné vytížení procesoru, výrazný nárůst datových toků apod.).
- Udržujte aktuální operační systém pravidelnými aktualizacemi a v co nejkratší době aplikujte všechny vydané bezpečnostní záplaty. Při aktualizaci operačních systémů serverů, aktivních prvků sítě a dalších obdobných zařízení dbejte pravidel pro testování a release management.
- Operační systémy, které nelze z provozních důvodů aktualizovat, umístěte do samostatného segmentu bez přístupu do internetu.
- Udržujte aktuální aplikační software, pravidelně kontrolujte verze instalovaného softwaru. U neaktuálního softwaru proveďte v rámci možností update. Zastaralé mohou být i verze použitých doplňků či modulů nebo firmware zařízení.
- Oddělte administrátorské účty pro správu a používejte speciální účty pro administraci systémů. Pro své ostatní pracovní aktivity (e-mail, web atd.) používejte běžný neprivilegovaný účet. Účet s oprávněním doménového administrátora používejte pouze ke správě Domain Controlleru (tzn. nepřistupujte jeho prostřednictvím na klientské stanice a servery).
- Doporučujeme zřídit nové administrátorské účty se stejným oprávněním jako administrator (admin, root) a původní účty zamknout (hesla k těmto záchranným účtům uložit do samostatných obálek do trezoru).

- Zabezpečte lokální administrátorské účty. Nastavte unikátní heslo na každé stanici, v prostředí Windows můžete využít například LAPS (Local Administrator Password Solution).
- Vynuťte používání silných hesel s ohledem na vyžadovanou složitost, délku a dobu platnosti. Zamezte opakovanému použití stejných hesel a používání slovníkových výrazů. Vynuťte změnu hesla, existuje-li podezření, že bylo kompromitováno.
- Odstraňte běžné uživatele z administrátorských skupin včetně lokálních administrátorských skupin.
- Při přístupu do internetu vynuťte ověřování uživatelů na firewallu nebo proxy serveru. Zkontrolujte a zakažte výjimky vytvořené v minulosti.
- Pokud to umožňuje Váš firewall, nastavte omezení přístupu uživatelů na internetové servery podle kategorií obsahu (phishing, malware, pornografie, hry, drogy, násilí apod.)
- Omezte přístup na sociální sítě pouze pro zaměstnance, kteří to mají v popisu práce.
- Pokud používáte Active Directory, vynuťte jednotné centrální politiky pomocí Group Policy.
- Při přístupu uživatelů pomocí VPN provádějte ověřování uživatelů vůči centrálnímu seznamu uživatelů (např. Active Directory).

1.3 Oblast ochrany dat

Vytvořte plán zálohování a obnovy dat (Disaster/Recovery plan), tento plán důsledně dodržujte, testujte a aktualizujte. Nezapomínejte na provádění Offline záloh. Offline zálohy dle rozsahu umísťujte na vhodná média a ukládejte mimo serverovnu. Tyto zálohy provádějte po v D/R plánu definovaných časových úsecích dle akceptovatelné časové ztráty dat. Obsahem D/R plánu musí být řetězec konkrétních kroků (scénář) pro obnovu dat. Musí obsahovat kontakty na odpovědné osoby, postup obnovy každého konkrétního prvku (servery, IS, síťový prvek apod.)

Typická struktura plánů obnovy:

- Umístění a popis záloh
- Pořadí a způsob obnovy jednotlivých komponent systémů
- Způsob ověření úspěšného obnovení dat ze zálohy
- Maximální časy obnovy
- Kontaktní údaje servisních organizací
- Metodika testování plánů obnovy

Doporučujeme udržovat aktuální verzi Disaster/Recovery plánu v tištěné podobě, aby mohl být aktivován i v případě výpadku systémů.

1.4 Oblast ochrany před podvodnými emaily

Jedním z nejčastějších vektorů kybernetických útoků (způsob infiltrace cílového zařízení) je phishing, případně spear-phishing. Způsobené škody se ročně globálně pohybují v desítkách až stovkách miliard korun. Sofistikovanost útočníků se přitom zvyšuje, a pro uživatele je stále těžší rozpoznat falešné e-maily nebo zprávy na sociální síti. Ty se stávají stále přesvědčivějšími a aktuálnějšími (využívají například pandemie koronaviru) a často obsahují přílohu se škodlivým kódem, kterou stačí otevřít, nebo odkaz na nakažené stránky, které stačí navštívit a informační systém oběti se dostane pod kontrolu hackerů. Zatímco o úspěchu útoku

může rozhodnout kliknutí jediného zaměstnance, obrana proti (spear)phishingu je výrazně složitější a vyžaduje technická, procesní a personální opatření.

Doporučené postupy obrany:

- Kontrolujte příchozí e-maily pomocí mechanismů Sender ID, SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) a DMARC (Domain-based Message Authentication, Reporting and Conformance) a blokujte podvržené zprávy. Tyto mechanismy nastavte i pro možnou kontrolu odchozích zpráv druhou stranou.
- Provádějte automatizovanou dynamickou analýzu obsahu e-mailů a webů prováděnou v sandboxu – hledejte podezřelé chování podle síťového provozu, tvorby nových souborů, úpravy stávajících souborů nebo změn konfigurace.
- Školte průběžně své uživatele na konkrétních příkladech. Školení provádějte prezenčně a formou elearningu.
- Monitorujte spamy ve své síti a včas upozorňujte uživatele na probíhající kampaně.
- Management Vaší organizace upozorněte na formy cílených útoků na konkrétní osoby managementu a prezentujte konkrétní příklady.

1.5 Oblast ochrany externích serverů

- Pro servery přístupné z internetu platí pravidla pro interní servery v podstatně zvýšeném měřítku (aktualizace operačního systému, aplikací, doplňků, modulů apod.).
- Kromě těchto pravidel omezte otevřené porty na těchto serverech na opravdu nejnutnější minimum.
- Zakažte nekompromisně jakýkoliv přímý přístup dodavatele aplikace na tyto servery. Přístup umožněte pouze přes centrálně řízenou VPN. Omezte přístup administrátorů pouze z určitých IP adres.
- Vynuťte šifrovanou komunikaci s klienty a zakažte používání protokolů SSL 2, SSL 3, TLS 1.0 a TLS 1.1. Nastavte používání pouze protokolů TLS 1.2 popř. TLS 1.3.
- Zvláštní péči věnujte emailovým systémům přístupným z internetu.

2 Reference

2.1 Doručené materiály a zdroje informací

- NÚKIB – doporučení pro administrátory 4.0
- NÚKIB – metodika k prověřování indikátorů kompromitace
- NÚKIB – SpearPhishing a jak se před ním bránit 2020
- Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) https://nukib.cz/
- Národní centrum kybernetické bezpečnosti (NCKB) https://www.govcert.cz/
- Národní centrum elektronického zdravotnictví http://www.nsez.cz/
- Ministerstvo zdravotnictví České republiky https://www.mzcr.cz/
- Ústav zdravotnických informací a statistiky ČR (ÚZIS ČR) https://www.uzis.cz/

2.2 Doručené nástroje

- Analýza vnějších zranitelností- https://www.shodan.io/
- Penetrační testy - https://pentest-tools.com/
- Zjištění provozovatele IP https://community.spiceworks.com/tools/ip-lookup/
- Zjištění škodlivé aktivity IP - https://www.abuseipdb.com/
- Databáze zranitelností https://nvd.nist.gov/vuln/