MINISTERSTVO ZDRAVOTNICTVÍ
ČESKÉ REPUBLIKY

Pokyn Ministerstva zdravotnictví ve věci kybernetické hrozby

V Praze dne 11. 12. 2019

PRAHA

Obsah

ÚVOD

Na základě rozsáhlého kybernetického útoku, který byl dnes veden vůči nemocnici v Benešově, vydává Ministerstvo zdravotnictví níže uvedený pokyn (v souladu s doporučením Federal Bureau of Investigation pod č. I-100219-PSA ze dne 2. 10. 2019), který je adresován všem organizacím v přímé řídící působnosti Ministerstva zdravotnictví.

Dokument je také veřejně publikován na webové adrese www.mzcr.cz pro případné využití dalšími organizacemi.

CO JE RANSOMWARE?

Ransomware je forma škodlivého kódu (malwaru), který šifruje soubory v počítači nebo serveru oběti a činí je nepoužitelnými. Kybernetičtí zločinci požadují výkupné výměnou za poskytnutí klíče k dešifrování souborů oběti.

Útoky Ransomware jsou stále cílenější, sofistikovanější a nákladnější, i když celková frekvence útoků zůstává konzistentní. Od začátku roku 2018 se výskyt širokých, nerozlišujících kampaní ransomware prudce snížil, ale ztráty z útoků ransomware se výrazně zvýšily.

JAK RANSOMWARE SE ŠÍŘÍ?

Počítačoví zločinci používají různé techniky k infikování systémů obětí ransomwarem. Kybernetičtí zločinci upgradují a mění své techniky, aby zefektivnili své útoky a zabránili odhalení.

Na základě dosavadních celosvětových zkušeností (informace FBI) jsou známy následující techniky k infikování obětí ransomwarem:

- **E-mailová phishingová kampaň:** Počítačový zločinec odešle e-mail obsahující škodlivý soubor nebo odkaz, který zavádí do počítače malware, když na něj příjemce klikne. Kybernetičtí zločinci historicky používali k nasazení svého škodlivého softwaru obecné,

široce založené spamové strategie, zatímco nedávné kampaně s ransomwarem byly cílenější. Zločinci mohou také ohrozit e-mailový účet oběti pomocí prekurzorového malwaru, který umožňuje počítačovým zločincům použít e-mailový účet oběti k dalšímu šíření infekce.

- **Zranitelnost protokolu vzdálené plochy** (dále "RDP"): RDP je patentovaný síťový protokol, který umožňuje jednotlivcům ovládat zdroje a data počítače přes internet. Kybernetičtí zločinci použili jak metody hrubé síly, tak techniku používající pokus-a-omyl k získání uživatelských pověření, a pověření zakoupená na trzích darknet k získání neoprávněného RDP přístupu k systémům obětí. Jakmile mají přístup k RDP, mohou zločinci nasadit do systémů obětí celou řadu malwaru - včetně ransomwaru.
- **Softwarová zranitelnost:** Počítačoví zločinci mohou využít slabých stránek zabezpečení v široce používaných softwarových programech, aby získali kontrolu nad systémy obětí a nasadili ransomware. Například kybernetičtí zločinci nedávno zneužili zranitelnosti ve dvou nástrojích pro vzdálenou správu, které používají poskytovatelé spravovaných služeb (MSP) k nasazení ransomwaru do sítí zákazníků alespoň tří MSP.

POKUD BYL SYSTÉM NAKAŽEN, JAK MÁM POSTUPOVAT DÁLE? NA KOHO SE MOHU OBRÁTIT?

NEDOPORUČUJE se výplata výkupného, protože to nezaručuje, že organizace znovu získá přístup ke svým údajům. Ve světě jsou známy případy, že i když bylo výkupné zaplaceno, nebyly poškozeným, dešifrovací klíče nikdy zaslány. Kromě toho kvůli obavám v šifrovacích algoritmech určitých variant malwaru nemusí být oběti schopny obnovit některá nebo všechna svá data ani s platným dešifrovacím klíčem.

Výplaty výkupného navíc mohou motivovat zločince k dalším útokům. Je proto nutné zohlednit rizika předtím, než se rozhodnete o dalším postupu. Pokud zaplatíte výkupné, prosím, VŽDY o této skutečnosti informujte Národní úřad pro kybernetickou bezpečnost (NÚKIB). Tím poskytnete kompetentním orgánům důležité informace, které jsou nezbytné ke sledování útočníků s ransomwarem.

JAK SE LZE BRÁNIT PROTI RANSOMWARE?

Nejdůležitější obranou jakékoli organizace proti ransomware je robustní systém záloh. Obnovení z nedávné zálohy by mohlo zabránit útoku ransomware na ochromení vaší organizace. ZÁLOHOVÁNÍ MUSÍ BÝT PROVEDENO PŘED VLASTNÍM KYBERNETICKÝM ÚTOKEM, ne později, kdy už může být pozdě.

Jak se ransomwarové techniky a malware stále vyvíjejí a stávají se sofistikovanějšími, ani ty nejrobustnější preventivní kontroly však nejsou zárukou proti zneužití. Proto je důležitá prevence a testování, aby se zajistila integrita citlivých údajů v případě kompromisu.

DOPORUČENÉ POSTUPY KYBERNETICKÉ OBRANY

- **Pravidelně zálohujte data a ověřte jejich integritu.** Zajistěte, aby zálohy nebyly připojeny k počítačům a sítím, které zálohují. Například je fyzicky uložte offline. V ransomwaru jsou zálohy kritické; Pokud jste infikováni, mohou být zálohy nejlepším způsobem, jak obnovit důležitá data.
- **Zaměřte se na osvětu a školení.** Protože cílem útočníků jsou koncoví uživatelé, měli by být zaměstnanci upozorněni na hrozbu ransomwaru a na to, jak je šířen, a proto je nutné zajistit školeni o zásadách a technikách informační bezpečnosti.
- **Opravujte operační systémy, software a firmware na zařízeních.** Po zjištění zranitelnosti by měly být opraveny všechny koncové body. To lze usnadnit prostřednictvím centralizovaného systému správy oprav.
- Zajistěte, aby byla **antivirová a antispywarová řešení** nastavena na automatickou aktualizaci a aby byly prováděny pravidelné kontroly.
- **Nastavte co nejnižší oprávnění pro přístup ke sdílení souborů, adresářů a sítí.** Pokud uživatel potřebuje přístup pouze ke čtení určitých souborů, neměl by mít k těmto souborům, adresářům nebo sdíleným položkám přístup pro zápis. Nakonfigurujte ovládací prvky přístupu s minimálním oprávněním.
- **Zakažte makro skripty ze souborů sady Office přenášených e-mailem.** Zvažte použití softwaru Office Viewer k otevírání souborů sady Microsoft Office přenášených e-mailem namísto plných aplikací sady Office Suite.
- **Implementujte zásady softwarového omezení (Group Policy) nebo jiné ovládací prvky,** abyste zabránili provádění programů v běžných umístěních ransomware, jako jsou dočasné složky podporující populární internetové prohlížeče, a programy komprese / dekomprese, včetně těch, které jsou umístěny ve složce AppData / LocalAppData.
- **Využijte osvědčené postupy pro používání protokolu RDP, včetně auditu vaší sítě u systémů používajících protokol RDP,** uzavření nepoužívaných portů RDP, použití dvoufaktorové autentizace, kdykoli je to možné, a protokolování pokusů o přihlášení protokolem RDP.
- **Implementujte seznam povolených aplikací.** Povolit systémům spouštět pouze programy známé a povolené bezpečnostní politikou (Group Policy).
- **Použijte virtualizované prostředí** k izolovanému spouštění prostředí operačního systému nebo specifických programů.
- **Rozdělte data podle jejich hodnoty a implementujte fyzické a logické oddělení sítí a dat pro různé organizační jednotky (virtuální sítě).** Například citlivá data z výzkumu nebo firmy by neměla být umístěna na stejném segmentu serveru a sítě jako e-mailové prostředí organizace.
- **Přistupujte na webové stránky pomocí firewallu nebo proxy serveru.** Vyžadujte interakci uživatele pro aplikace koncových uživatelů komunikující s webovými stránkami nezařazenými do síťového proxy nebo brány firewall. Například požadujte, aby uživatelé zadali informace nebo zadali heslo, když jejich systém komunikuje s webem nezařazeným do proxy nebo brány firewall.