Ransomware

Ransomware (složenina anglických slov *ransom* – výkupné a *software*) je druh škodlivého softwaru, který útočníci používají k vydírání obětí. Po infiltraci do systému zašifruje soubory nebo uzamkne obrazovku a následně zobrazí zprávu s požadavkem na zaplacení částky, obvykle v kryptoměnách (např. Bitcoin), výměnou za dešifrovací klíč.

Jak ransomware funguje? (Průběh útoku)

Moderní útoky (zejména ty cílené na firmy) probíhají v několika fázích:

1. **Infiltrace:** Nejčastěji skrze phishingový e-mail, zneužití zranitelnosti (Zero-day) nebo přes nezabezpečený vzdálený přístup (RDP).
2. **Šíření (Lateral Movement):** Malware se snaží infikovat další počítače a servery v síti, aby maximalizoval škody.
3. **Exfiltrace dat (Dvojité vydírání):** Útočníci nejprve data ukradnou a až poté je zašifrují. Vyhrožují jejich zveřejněním, i když má oběť zálohy.
4. **Šifrování:** Použití silných algoritmů (AES nebo RSA), které nelze bez klíče prolomit.
5. **Vyděračská zpráva:** Instrukce k platbě, často s časovým limitem (odpočet).

Typy Ransomwaru

- **Crypto-ransomware:** Nejobvyklejší typ. Šifruje cenné soubory (dokumenty, fotky, databáze), ale systém zůstává částečně funkční.
- **Locker-ransomware:** Uzamkne celý přístup k operačnímu systému. Uživatel vidí pouze obrazovku s výzvou k platbě.
- **RaaS (Ransomware as a Service):** Model, kdy tvůrci malwaru „pronajímají“ svůj kód ostatním útočníkům za podíl ze zisku.

Strategie obrany a prevence

Obrana proti ransomwaru vyžaduje vícevrstvý přístup:

- **Zálohování (Pravidlo 3-2-1):** 3 kopie dat, 2 různá média, 1 kopie **offline** (nepřipojená k síti). Offline záloha je jedinou 100% ochranou proti zašifrování záloh.
- **Pravidelné aktualizace:** Záplatování systému proti zranitelnostem.
- **E-mailové zabezpečení:** Filtrování příloh a ochrana proti phishingu.
- **Endpoint Protection (EDR):** Pokročilé antiviry, které sledují podezřelé chování (např. hromadné přejmenovávání souborů).
- **Segmentace sítě:** Zabránění malwaru v šíření z jednoho nakaženého PC na zbytek firmy.

Platit, nebo neplatit?

Bezpečnostní experti a policie (např. FBI, Europol) **důrazně nedoporučují platit**.

- **Žádná záruka:** Zaplacení nezaručuje, že útočník klíč pošle.
- **Financování zločinu:** Peníze motivují útočníky k dalším útokům.
- **Snadný cíl:** Pokud jednou zaplatíte, stanete se pro útočníky označeným „platičem“ a pravděpodobně zaútočí znovu.

> **Projekt No More Ransom:** Existuje globální iniciativa **NoMoreRansom.org**, kde bezpečnostní firmy zveřejňují dešifrovací klíče pro starší nebo špatně napsané verze ransomwaru. Před jakýmkoliv rozhodnutím je dobré zkontrolovat, zda pro daný kmen neexistuje dešifrátor zdarma.

— **Viz také:** Zero-day útok, Šifrování, SIEM, Offline zálohování