Acronis

Ransomware, dá se proti němu vůbec bránit?

Aleš Hok

PM Acronis ve společnosti ZEBRA SYSTEMS

+420 776 008 731, ales.hok@acronis.cz

WILLIAMS RACING
OFFICIAL PARTNER

Bezpečnostní zpráva Microsoft Security Intelligence Report 2019 říká:

„Počet útoků, při nichž útočníci zašifrují data oběti a vyhrožují, že je smažou, pokud oběť nezaplatí výkupné, klesl vloni o 73 %. Česká republika a Slovensko patří mezi nejméně ohrožené země s výskytem o polovinu nižším, než je celosvětový průměr.“

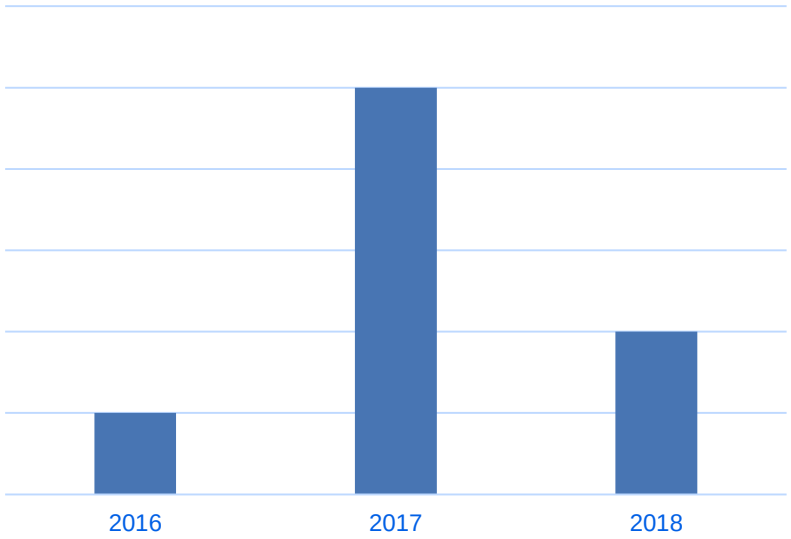
Takže bychom měli být spokojeni …

… přesto finanční škody způsobené ransomwarem setrvale rostou

Jak je to možné?

… hodně útoků, mále škody

- 2017 několik velmi masivních ransomwarových útoků šířených emailem (WannaCry, Petya, Bad Rabbit).
- Malé částky vyžadovány po hodně subjektech. Maskovaná sabotáž …
- Emaily nebyly zacíleny na náš region. Emaily nebyly přeložené. Ani v angličtině častokrát nevypadaly příliš důvěryhodně.
- V roce 2018 se tak masivní útoky nezopakovaly. Velmi se rozšířil cryptojacking.



Ilustrační graf

Od masivních k cíleným útokům

- Vyděrači se nyní specializují na cílené útoky zaměřené na důležité, úspěšné a bohaté organizace.
- Méně práce s větším ziskem (pokud je dostatečné know how)
- Například v Norsk Hydro (3/2019 / ransomware LockerGoga).
- Zakryptování je velmi snadný způsob jak z poškozených organizací rychle získat peníze. Motivem není ublížit, ale zisk.

Co se čeká do budoucna

- Hromadné necílené emailové útoky. Těžko předvídat. V případě globálních útoků je riziko ohrožení v ČR a SR poměrně nízké.
- Bude pokračovat trend konkrétně cílených útoků formou hackingu především na úspěšné a bohaté organizace.
- Konkrétně cílené emailové útoky. Na konkrétní osoby (oddělení). Perfektně vyladěné a důvěryhodné emaily v daném jazyce.

Konkrétně cílené emailové útoky

- Specializace emailových útoků na odvětví organizace a zaměření jednotlivců
- Věrohodně vypadající fake životopis na email na konkrétního HR manažera
- Fake objednávka poslána konkrétnímu vedoucímu obchodu
- Fake faktura po splatnosti s výhružkou poslána na hlavní účetní
- Výše postavení zaměstnanci budou hlavní iniciátoři kryptování. Jejich seznamy a kontakty bývají často veřejně dostupné. Znát oběť = větší šance na úspěch

Případová studie Armaturka Krnov

- Zálohovací řešení Acronis od 2016
- Několik zakryptování ze stejného stroje
- Přesná příčina nakonec nezjištěna
- Po obnovení propuklo šifrování znova
- Pravděpodobně trojan / backdoor
- Usídlený dlouhodobě v daném stroji
- Chytrý ransomware – vyčkával
- Pomohla
- Dnes bychom využili aktivní ochranu

Možnosti obrany - obecně

- Přitvrdit v emailové ochraně a filtrování
- Zamezit odesílání emailů z jiného než vlastního serveru
- Nedávat zbytečná práva uživatelům
- Neposkytovat uživatelům zbytečné přístupy
- Poučit a pravidelně školit uživatele
- Provádět penetrační testy (ideálně jiným subjektem)
- A využívat **aktivní** i pasivní ochranu

Zálohovat, zálohovat, zálohovat

- Když selže všechno ostatní, pomůže pouze obnovení. Záloha je největší nepřítel ransomwaru.
- Záloha není jen záchranný člun, který zmírní škody (v námořnické terminologii nenechá utopit tolik lidí).
- Záloha je nástroj, který vaši loď vyzvedne ze dna a opraví ji tak, že loď může zase pokračovat v cestě.

Důkladně schovat zálohy

- Zálohy musí být pro ransomware absolutně nedostupné. Žádný uživatel, proces ani služba s výjimkou zálohovacího řešení nesmí mít přístup k zálohám.
- Vyčleňte pro zálohy zabezpečený prostor
- Využít lze také střídání a odpojování úložišť, robotické pásky

Ideálně ukládat kopie záloh také off site

- Klasické pravidlo 3 - 2 - 1
- Aktualizujeme na 3 - 2 - 1 - 1

3 - Kopie dat, z toho jedna jsou zdrojová data

2 - Různé typy úložišť

1 - Záloha off site

1 - Alespoň jedna ze záloh je nemanipulovatelná

Pozor, není cloud jako cloud

Disaster Recovery - když záloha nestačí

- Pokud nejste ochotni nebo nemůžete tolerovat výpadky v řádu hodin, použijte řešení pro Disaster Recovery.
- Možnost rychle zprovoznit kritické systémy z vlastní DR lokality nebo v cloudu.
- Aktuální stavy systémů se nakonec plynule přenesou zpět do produkčního prostředí.
- Nedochází ke ztrátě dat. Výpadky jsou minimalizovány.

Acronis

WILLIAMS RACING
OFFICIAL PARTNER

Děkuji za pozornost

Aleš Hok
+420 776 008 731, ales.hok@acronis.cz
www.acronis.cz