ALISON

Vydieranie, výkupné a údaje o pacientoch na predaj. Fakt zlý rok pre zdravotníctvo

- Najhoršie útoky
- Dva míľniky práve v tomto roku
- Cena za jeden ukradnutý záznam
- A situácia na Slovensku

Počas pandémie vydieračské útoky a praktiky narástli až exponenciálne. Priemerné výkupné v roku 2020 sa zvýšilo na 234 000 dolárov, pričom ešte v treťom štvrťroku 2019 to bolo 41 000 dolárov.

Na vzostupe je takzvaný skrytý ransomvér, ktorý zneužíva šifrovanie webového protokolu SSL. Jeho výskyt narástol od marca do septembra 2020 o viac ako 260 percent. Hlavným cieľom sa stalo zdravotníctvo a hneď po ňom financie a poisťovníctvo, priemyselná výroba, vláda a služby. Na siete zdravotníckych zariadení cielila viac ako štvrtina všetkých útokov.

Medzinárodné zdravotnícke organizácie sa stali frekventovaným cieľom útokov s tematikou COVID-19, keďže v ich prevádzke sa vyžaduje akútne nasadenie, nemajú čas vyjednávať a väčšinou sú tak nútené platiť výkupné.

Bod zlomu

Za najväčší útok v histórii malvéru sa považuje WannaCry, ktorý v roku 2017 zablokoval viac ako 250-tisíc počítačov v 150 krajinách, pričom zasiahol najmä Rusko, Ukrajinu, Indiu a Taiwan. S neuveriteľnou silou napadol aj sieť 48 regionálnych nemocníc v Spojenom kráľovstve, kde ochromil počítače, skenery, chladiace zariadenia zásobníkov krvi a ďalšie zariadenia. A ak sa aj zlomyseľne hovorí, že hackeri neútočia na Slovensko preto, lebo ho nevedia nájsť na mape, tak nitrianska fakultná nemocnica sa práve v tomto roku stala kontrapríkladom. Vírus napádal počítače cez operačný systém Microsoft Windows, ak nemal používateľ aktualizovanú verziu alebo ho používal po skončení platnosti. Autorstvo útoku sa pripisuje Severnej Kórei.

Regionálnu bezpečnostnú letargiu či rozpočty v našom regióne po dvoch rokoch nabúral útok na benešovskú nemocnicu. Vydieračský softvér blokoval prístroje a útočníci žiadali platbu v kryptomenách. Nemocnica výkupné údajne nezaplatila, z kybernetického útoku sa však dostávala mesiac a celkové škody oficiálne vyčíslila na 50 miliónov českých korún. A pritom útok sa začal otvorením jedného mailu.

Zhoršuje sa to

Pocit ohrozenia a panika vyvolané pandémiou priniesli smršť phishingových kampaní či falošné ochranné pomôcky a úhrady neexistujúcim dodávateľom. Kybernetické organizované skupiny

skrátili obdobie medzi počiatočnou infekciou ransomvéru a aktiváciou útoku, pretože nečakali na ideálny okamih na spustenie útoku, ale útočili čo najskôr, aby maximalizovali zisky.

Medzi tie lepšie správy patrí tá, keď v marci oznámil najväčší prevádzkovateľ nemocníc v Európe AP-HP Paris Hospital Authority, že „ustál" útok, ktorý sa silou a nasadením počíta medzi najväčšie v roku 2020. K menej šťastným obetiam v tejto vlne však patrili české nemocnice. Útok na databázové systémy Univerzitnej nemocnice v Brne ochromil nielen samotné systémy, ale aj celú prevádzku na niekoľko dní. Krajská nemocnica v Karlových Varoch zaznamenala v apríli útoky dva dni po sebe. Ostravská nemocnica už otvorene priznáva, že odráža phishingové útoky často. Reaguje na to zabezpečením ochrany infraštruktúry a nadštandardným zálohovaním, čiže – dve geografické lokality a aspoň dva druhy zariadení.

Do histórie sa rok 2020 zapíše aj prvou obeťou. Útok ransomvéru spôsobil zlyhanie systémov v Univerzitnej nemocnici v Düsseldorfe, takže pacientka, ktorej nemohli poskytnúť urgentne pomoc, zomrela pri prevoze. Nemocnica uviedla, že zdrojom problému bol útok na slabé miesto v „široko používanom komerčnom doplnkovom softvéri", v dôsledku čoho systémy postupne padali. Hackeri vytvorili ešte ďalší nechcený míľnik. Chceli údajne zaútočiť na Univerzitu Henricha Heineho, ku ktorej je nemocnica pridružená. Výzvu na úhradu totiž adresovali všeobecne. V tej chvíli bolo zašifrovaných 30 serverov. Keď polícia informovala, že je zasiahnutá nemocnica, útočníci stiahli pokus o vydieranie a poskytli kľúč na dešifrovanie údajov.

A kde je problém?

V kliknutí na lákavý mail alebo v nepozornosti. Najčastejšie zneužitými značkami v phishingových útokoch sú Microsoft, PayPal a Google. Profesionáli sú však v hodnotení neľútostní – problém nie je primárne v neznalosti zdravotníckeho personálu, účtovníčok, administratívy či personálneho oddelenia. Phishingový mail nemá vôbec čo prejsť do siete! Ak sa tak už stalo, znamená to, že už zlyhal prvý stupeň ochrany a začína sa diať sled udalostí na rôznej úrovni. Žiadne zariadenie si však s ohrozením nedokáže poradiť samo, a preto sa vyhodnocuje ochrana perimetra, no najmä ochrana na koncovom zariadení.

Kybernetický útok môže zaznamenať správca v systéme ako zvýšenú aktivitu. Nová generácia ransomvéru najprv vyhľadáva cenné dáta a skopíruje ich a až následne ich šifruje. Po opakovaných šifrovaniach pošle hlášku, výstrahu a výzvu na platbu. Zvyčajne je to 72 hodín. Keď platba prebehne, hacker pošle kód na dešifrovanie dát. Alebo môžete oželieť dáta. Takže?

Dáta nad zlato

Krádež osobných údajov potvrdila v septembri sieť psychiatrických centier Vastaamo, ktorá má vo Fínsku približne 40-tisíc pacientov. Incident sa stal zhruba pred dvoma rokmi, keď útokom na CRM systém hackeri získali citlivé údaje o pacientoch. Žiadali výkupné 450-tisíc eur, medzičasom však vylákali platby aj od samotných pacientov vo výške od dvesto do päťsto eur. Bezpečnostní experti

uvádzajú, že desaťgigabajtový dátový súbor obsahujúci odkazy medzi dvetisíc pacientmi a ich terapeutmi sa objavil na dark webe.

Podobný problém riešila v júni aj spoločnosť Magellan Health zaradená do rebríčka Fortune 500. Spoločnosť bola zasiahnutá útokom ransomvéru a únikom osobných údajov v apríli 2020. Zdravotnícky gigant potvrdil, že sofistikovaným kybernetickým útokom bolo postihnutých asi 365-tisíc pacientov. Hackeri sa dostali k informáciám o liečbe, informáciám o účte zdravotného poistenia, rovnako získali aj e-mailové adresy, telefónne čísla a fyzické adresy pacientov.

Cena za uniknutý záznam

Zdravotníctvo má už desiaty rok po sebe najvyššie priemerné náklady spojené s únikom údajov. V porovnaní s rokom 2019 ide opäť o nárast desať percent. Základným typom odcudzeného záznamu sú „osobne identifikovateľné informácie“ o klientoch, čo uviedlo až osemdesiat percent organizácií. Informácie z takéhoto záznamu umožňujú identifikáciu osoby. Odcudzenie jedného takéhoto záznamu stálo spoločnosti v priemere 150 amerických dolárov.

Cena dátových únikov sa tvorí na základe otázok, ktoré mapujú, aké finančné prostriedky sa vynaložili na aktivity na odhalenie a okamžitú reakciu na porušenie ochrany údajov. Vplyv na finančné náklady mali bezpečnostné opatrenia implementované pred incidentom, určenie príčin úniku údajov, čas, ktorý organizácie potrebovali na zistenie a zvládnutie incidentu, ale aj odhadované náklady na prerušenie podnikania a stratu zákazníkov v dôsledku úniku údajov.

Útoky, poruchy, nedbanlivosť

IBM Report rozdeľuje hlavné príčiny úniku dát do troch hlavných kategórií. Nadpolovičnú väčšinu incidentov (52 %) spôsobuje zlomyseľný útok. Druhou najčastejšou príčinou úniku dát boli poruchy (25 %) a trojicu uzatvára zlyhanie ľudského faktora (23 %).

Odvetvia sa líšia aj podľa toho, aké príčiny najčastejšie spôsobujú dátové úniky a tým aj škody. Technológie, doprava, maloobchod a financie mali najvyššie percento škodlivých útokov. Zábavný, verejný sektor a spotrebný priemysel mali najvyššie percento úniku dát spôsobených ľudskou chybou. Systémové chyby boli častejšie hlavnými príčinami úniku vo výskume, verejnom sektore a v doprave.

A situácia na Slovensku?

Celková úroveň zabezpečenia jednotlivých nemocníc a ich schopnosti odolať ransomvérovému útoku je spravidla nedostatočná a nepostačuje na to, aby boli nemocnice schopné postaviť sa profesionálnym hackerom 24 hodín denne. Chýbajú bazálne bezpečnostné opatrenia, čo prestavuje vysoké riziko ransomvérového útoku.

Celý sektor trpí významnou podinvestovanosťou v oblasti kybernetickej bezpečnosti z hľadiska jednotlivých oblastí, či už funkcií a technológií, no najmä ich personálneho zabezpečenia.

ALISON

Tak si skúsme najprv odpovedať na tieto otázky:

- Postupovať naďalej v čiastkovom riešení kybernetickej bezpečnosti v jednotlivých nemocniciach alebo sa prikloniť k rezortnému riešeniu?
- Aké investičné a operatívne prostriedky bude potrebné vynaložiť na oblasť kybernetickej bezpečnosti v jednotlivých nemocniciach?
- Alternatívne – aké investičné a operatívne prostriedky bude potrebné vydať na rezortné riešenie?
- Ako dlho bude trvať, než dokážeme zabezpečiť kybernetickú bezpečnosť všetkým nemocniciam v rámci rezortu?