HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 23. – 25. FEBRUÁRA 2024

Kúpiť bitcoiny, alebo si poplakať?

ANKETA

Pýtame sa profesionálov: Ako budete reagovať, keď vám príde blízky človek zúfalo oznámiť, že má zašifrované alebo zmiznuté všetky fotky v počítači a po zaplatení výkupného ich dostane späť?

Jaroslav Ďurovka,
riaditeľ
Národné centrum kybernetickej bezpečnosti SK-CERT

Prvá rada je rovnaká bez ohľadu na to, kto čelí ransomvéru – nepodľahnúť panike a neplatiť výkupné. Platba nemusí stačiť. Je vysoko pravdepodobné, že šifrovacie kľúče vám útočník nepošle alebo bude s vydieraním pokračovať. Vždy je dobré obrátiť sa na bezpečnostných expertov, ktorí vedia pomôcť s analýzou toho, čo sa stalo, ale aj s obnovou dát. Ďalším správnym krokom je nahlásiť incident na NBÚ a prípadne podať aj trestné oznámenie na políciu. Najlepšie je však predchádzať takýmto incidentom – učiť sa, na čo si dávať pozor, a dodržiavať pravidlá kybernetickej bezpečnosti.

Ivan Makatura,
generálny riaditeľ
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Snažil by som sa vysvetliť, že ani zaplatením výkupného väčšinou svoje dáta späť nezíska. Potom zistiť, aké staré sú zálohy jeho dát. A ak žiadne zálohy nemá, potom mu už len zavolať záchranku. Rovnako ako po nakazení biologickým vírusom by bolo zbytočné začať chorého človeka presviedčať o potrebe prevencie.

Henrich Šnajder,
manažér IT bezpečnosti
Orange Slovensko

Ak by boli dáta zašifrované a používateľ ich nemal zálohované, zistil by som použitú verziu ransomvéru a odzálohoval by som všetky zašifrované dáta. Niekedy je dôležité dostať sa k niektorým originálnym dátam, napríklad k tým, čo boli odoslané na iné zariadenie. Existuje šanca, že dáta bude možné dešifrovať ihneď alebo v budúcnosti pomocou dešifrovacích nástrojov. Ako druhé by som poradil, ako sa efektívne zabezpečiť proti ransomvérovým hrozbám do budúcnosti.

Katarína Kročková,
odborníčka na ochranu osobných údajov
Kročka & Partners

Všetkých svojich blízkych som poučila o tom, ako sa majú chrániť v online priestore. Avšak, ak by nastala situácia „Houston, máme problém!“, určite by som blízku osobu upokojila. Zistili by sme čo najviac informácií o tom, čo sa presne stalo a akým spôsobom, o aký druh fotografií ide a, samozrejme, či existuje záloha. Odporučila by som jej nekomunikovať s útočníkom, neplatiť mu výkupné.

Ivan Kopáčik,
bezpečnostný expert
Gordias

Blízky človek bude asi v šoku, takže zhruba: 1. Upokojím 2. Zistím rozsah škôd 3. Zistím, či neexistuje záloha napríklad v cloude. 4. Vysvetlím, že platiť určite nie, lebo je to zbytočný pokus. 5. Presmerujem na špecialistu, ktorý sa riešením tohto typu incidentov rutinne zaoberá.

Marián Illovský,
audítor kybernetickej bezpečnosti
Auditori.it

Pokoj, však určite máš nastavené zálohovanie. Pravidelné zálohovanie dôležitých dát mimo zariadenia, kde sú primárne uložené, je dnes už štandard.

Andrej Žucha,
generálny riaditeľ
ALISON Slovakia

Máš zálohu? Ak nie, tak sa so všetkým rozlúč.

Tomáš Zaťko,
CEO, etický hacker
Citadelo

Pokojne vysvetlím, že výpalné platiť nebudeme a dáta obnovíme zo zálohy. Verím, že moji blízki už základnú hygienu kybernetickej bezpečnosti zvládajú. Efektívne zálohovanie je jej súčasťou.

Michal Srnec,
vedúci oddelenia informačnej bezpečnosti
Aliter Technologies

Očakávanie, že zaplatením výkupného sa automaticky zaručí vrátenie dát, je viac než otázne. Pravdepodobnosť úspechu je ako hod mincou. Vysvetlil by som, prečo nie je dobrý nápad platiť za dešifrovanie, a skôr by som sa zameral na hľadanie technickej odpovede. Napríklad, ako zistiť, o aký typ ransomvéru ide, či existujú dostupné dešifrovacie kľúče alebo návody na jeho rozlúštenie. No aj pri tejto ceste sú šance na úplné získanie všetkých dát stále len fifty-fifty.

Jana Puškáčová,
manažérka útvaru Informačná bezpečnosť
MOL IT & Digital Slovensko

Klebety a fotky na internete sú ako perie. Keď ich raz rozšíriš, viac ich pod kontrolu nedostaneš. Ani za peniaze.

Jakub Berthoty,
advokát
Dagital Legal

Samozrejme, na počkanie by som všetko odšifroval.

Tomáš Valenta,
riaditeľ
Check Point Software Technologies na Slovensku

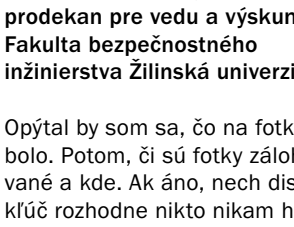
Že by pomohlo zaplatiť a do pár minút bude všetko naspäť bez akýchkoľvek následkov? Neverím, že by to niekto myslel vážne. Takže: Neplatiť, neplatiť a ešte raz neplatiť. No a, samozrejme, čo najskôr inštalovať kvalitnú ochranu.

Ján Golais,
poradca bezpečnosti
Slovak Telekom

Vidíš, ja som ti to vravel... A v žiadnom prípade nech neplatí. Nech si spustí cez restor dát z natívnych funkcií operačného systému. A tiež by som mu pripomenul dôležitosť zálohovania a obnovy dát.

Jaroslav Ďurovka,
riaditeľ
Národné centrum kybernetickej bezpečnosti SK-CERT

Prvá rada je rovnaká bez ohľadu na to, kto čelí ransomvéru – nepodľahnúť panike a neplatiť výkupné. Platba nemusí stačiť. Je vysoko pravdepodobné, že šifrovacie kľúče vám útočník nepošle alebo bude s vydieraním pokračovať. Vždy je dobré obrátiť sa na bezpečnostných expertov, ktorí vedia pomôcť s analýzou toho, čo sa stalo, ale aj s obnovou dát. Ďalším správnym krokom je nahlásiť incident na NBÚ a prípadne podať aj trestné oznámenie na políciu. Najlepšie je však predchádzať takýmto incidentom – učiť sa, na čo si dávať pozor, a dodržiavať pravidlá kybernetickej bezpečnosti.



Tomáš Loveček,
prodekan pre vedu a výskum Fakulta bezpečnostného inžinierstva Žilinská univerzita

Opýtal by som sa, čo na fotkách bolo. Potom, či sú fotky zálohované a kde. Ak áno, nech disk či kľúč rozhodne nikto nikam hneď nepripája, keďže väčšina z nás by si určite chcela pozrieť, o čo prišla. V súvislosti s platbou je odpoveď jasná, ale ruku na srdce – kto by to za určitých okolností nezvažoval. S informáciami vzhľadom na ohlásenie, odpojenie, reinštaláciu, update, zmeny hesiel by som obeť útoku v tú chvíľu netrápil. V každom prípade fotokniha je istota.

Ján Adamovský,
riaditeľ bezpečnosti
Slovenská sporiteľňa

Spoločne si sadneme, nájdeme spôsob, ako sa z roviny emócií dostať do roviny faktov. Vysvetlíme si, že platenie výkupného ako finančná podpora kriminálnych aktivít nie je cesta. Pozrieme sa na to, či má zálohy. Zistíme, ako k strate prišlo. Ak sa obnova fotografií podarí, všetko dobre dopadlo. Ak nie, svet sa nekončí. Ľudia sa učia na cudzích, ale často aj na vlastných chybách.

Martin Oczvirk,
riaditeľ odboru informačnej bezpečnosti a certifikácie Úrad na ochranu osobných údajov

Určite by som poradil neplatiť žiadne výkupné. Garancia vrátenia fotiek neexistuje. Ak nemáme zálohu alebo nás fotky stavajú do chúlostivej situácie, môžeme si spolu jedine poplakať. Aby sme sa takejto situácii vyhli, treba dodržať nasledovné minimum: pravidelne aktualizovať systém, zálohovať a šifrovať údaje a mať antivírus.

Tomáš Hettych,
viceprezident
ISACA

Ak je počítač napadnutý ransomvérom, tak prvotná reakcia je upokojiť známeho a presvedčiť ho, aby nič nezaplatil. Zaplatenie výkupného väčšinou nikam nevedie. Následne overiť verziu malvéru a pokúsiť sa zohnať kľúč na dešifrovanie. Väčšina kľúčov sa po určitom čase publikuje. Ak sú fotky a súbory len zmazané, tak použijem špecializovaný nástroj na obnovu a s vysokou pravdepodobnosťou ich obnovím.

Roman Čupka,
hlavný konzultant
Progress, CSO Istrosec

Ak neexistuje „dešifrovací kľúč“, prejavím najlhbšiu sústrasť nad stratou dát a odporučím výkupné radšej investovať do predplatenej cloudovej služby, osobného dátového úložiska a nového počítača, či radšej dvoch, a to vrátane VPN služby. Poskytnem radu, ako správne automatizovane a pravidelne dáta zálohovať a v prípade obdobných prípadov ich aj jednoducho obnovovať. A to nielen fotky, súbory a citlivé informácie ale aj systémové nastavenia počítača, či mobilného telefónu. Posledná rada bude zmeniť všetky používané heslá. Plus pár jednoduchých typov ako sa v digitálnom priestore správať obozretne a zodpovedne.

Timea Tomčová,
manažérka informačnej bezpečnosti
Poisťovňa Union

V prípade, že už je na osvetu neskoro a došlo k úniku, prípadne zašifrovaniu dát a útočník žiada výkupné, radím neplatiť. Pri platbe nie je istota, že bude dodržaná dohoda zo strany útočníka, a škoda môže byť vo výsledku ešte väčšia.

Július Selecký,
senior technický špecialista ESET

V prvom rade ho upokojím a odporučím mu neplatiť. Následne mu pripomeniem našu dávnu debatu o dôležitosti zálohovania. Takže môj blízky človek si pripojí externý disk, na ktorý už medzičasom zabudol, a obnoví si tie fotografie. Respektíve si ich obnoví z cloudu.

Michal Sekula,
bezpečnostný konzultant
Eviden Slovakia

Ak je to naozaj môj blízky človek, tak má spravené zálohy a v tom prípade je riešenie pomerne jednoduché. Rozhodne však neodporúčam platiť výkupné. Nielen preto, že to páchateľov len povzbudí, ale často sa po zaplatení dáta nedajú obnoviť, prípadne útočníci kľúč ani neposkytnú. Útechou môže byť, že ide „len“ o fotky, a nie napríklad o citlivé dáta z podnikania. V každom prípade je to pomerne drahý spôsob, ako si uvedomiť dôležitosť zálohovania.

Marek Madžo,
technický riaditeľ centra kybernetickej bezpečnosti void SOC
Soitron

Reagoval by som rovnako ako pri zákazníkoch – podľa incident response plánu pri ransomvéri. Prvým krokom je analýza a zhodnotenie situácie, ktorá nemusí byť vždy taká zlá, ako sa zdá na prvý pohľad, niekedy je aj horšia. Odporúčam neplatiť výkupné, čiže nepodporovať útočníkov a zamerať sa v paralelných streamoch na obnovu dát, investigáciu rozsahu a príčiny incidentu s návrhom a prijatím opatrení.

Peter Dufek,
manažér kybernetickej bezpečnosti
Penta Hospitals SK

Najskôr by som asi prejavil úprimnú ľútosť a potom vysvetlil, že takému prísľubu netreba veriť, rozhodne nič neplatiť, lebo to nie je záruka vrátenia. Nikdy ich nezíska späť, aj keby bol ochotný zaplatiť. Ako ďalší krok by som odporučil vykonať potrebné kroky, od výmeny disku či systému cez inštaláciu antivírusu, zabezpečenie domácej siete až po pravidelné zálohovanie. Najlepšou školou je vlastná skúsenosť!

Pavel Nechala,
advokát
Nechala and partners

V prvom rade určite neplatiť výkupné a odpojiť okamžite od siete všetky napadnuté zariadenia. Obnovenie záloh, ako aj ďalšie kroky budú vyžadovať profesionálnu pomoc. A len čo sa primárny problém vyrieši, je potrebné sa vrátiť k základom. Teda položiť si otázku, ako zlepšiť odolnosť proti kybernetickým hrozbám.

Marián Trizuliak,
architekt kybernetickej bezpečnosti
Západoslovenská distribučná

Nepredpokladám, že odpoveď je určená kolegom z brandže, skôr kamarátovi, a keďže ho dobre poznám, tak – nehovoril som ti stokrát, že nemáš klikať na všetko, čo máš v mailoch? Alebo nebodaj ťa zase raz zlákala cracknutá hra? Super, máš ponaučenie. A ďakujem za hodiny strávené reinštaláciou počítača.