HN obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

PIATOK – NEDEĽA 23. – 25. FEBRUÁRA 2024

Odborná spolupráca

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

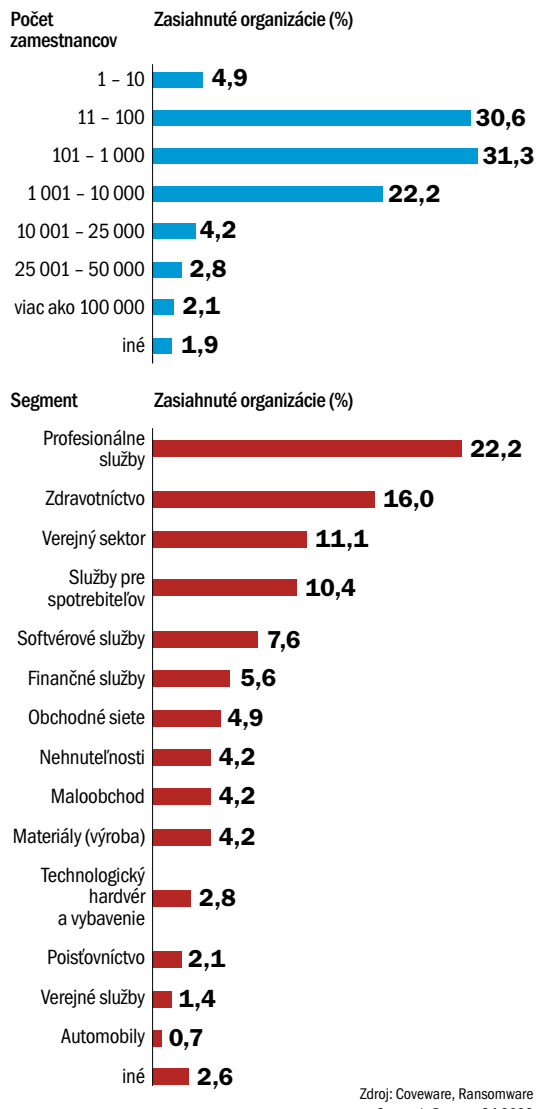
SK CERT NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

Ransomvér? Vaše obavy sú oprávnené

Automatizované útoky zvyšujú frekvenciu a cieľom sú firmy všetkých veľkostí.

SNÍMKA: DREAMSTIME

Obete ransomvérových útokov (Q4 2023)



Zdroj: Coveware, Ransomware Quarterly Reports Q4 2023

TÉMA

Ransomvérové útoky sa robia so šifrovaním aj bez šifrovania. Útočníci preskúmajú, čo má akú hodnotu, ukradnú, čo sa dá, a potom začnú vydierať. Vás aj vašich zákazníkov.

Zničujúce kybernetické útoky sa zvyčajne začínajú cez víkendy a sviatky. V skutočnosti sa však začali dávno pred tým, ako na to prídete.

Detegovať ransomvérového „votrelca“ v systéme alebo v sieti trvá priemerne 207 dní. Vo väčšine prípadov však útočníkom stačí osemdesiat dní, aby získali, čo potrebujú.

Nočná mora

Nočná mora kyberbezpečnosti minulého roka sa oficiálne začala počas májového víkendu.

Zločinci zneužili zraniteľnosť v aplikácii na prenos súborov MOVEit. Išlo o takzvanú zero-day zraniteľnosť, kde nie sú vydané bezpečnostné záplaty. Keďže aplikácia je široko používaná, útoky boli masívne.

Výrobca okamžite vydal bezpečnostné záplaty a varovania, ale útok sa valil ako cunami. Útočníci túto zraniteľnosť poznali viac ako dva roky a mali dosť času, aby údaje v napadnutých organizáciách skúmali a kradli.

Tisícky cieľov

Obeťami sa stali vládne agentúry, školy, univerzity, zdravotnícke zariadenia, médiá, banky, letecké spoločnosti, zábavný priemysel či účtovnícke korporácie. Podľa monitorovania Emsisoft to bolo viac ako 2 600 postihnutých organizácií.

K útokom sa prihlásil známy ransomvérový gang Cl0p. V tomto prípade však údaje nešifrovali a rovno žiadali výkupné. Za to, že nezverejnia získané údaje. Experti odhadujú, že doteraz mohli získať výkupné 75 – 100 miliónov dolárov.

Červené čísla

V súvislosti s kauzou „hack MOVEit“ sa odhaduje, sa, že uniklo 83 miliónov údajov. Ak mienkotvorný report IBM uvádza priemerné náklady na narušený údaj 165 dolárov, sumárne škody sa blížia k 14 miliardám dolárov.

Doteraz najvyššiu škodu – desať miliárd dolárov – vykazuje ransomvér NotPetya, ktorý spôsobuje nedostupnosť systémov a údajov.

V reakcii na závažnosť útoku hack MOVEit vyhlásila vláda USA odmenu desať miliónov dolárov za akékoľvek informácie vedúce k zatknutiu a odsúdeniu páchateľov.

Nový trend na scéne

Jakub Souček, výskumník spoločnosti ESET, považuje tento ransomvérový útok za míľnik, keďže „aj bez šifrovania ukazuje rozvíjajúce sa techniky a potenciálny vplyv kybernetických útokov“.

Prípadne sa pri útokoch používa wiper, čiže softvér, ktorý údaje u obete úplne zničí.

„Ransomvér už nie je len nejaký druh počítačového vírusu. Je to celý škodlivý ekosystém zložený z organizovaných skupín, postupov, nástrojov a dokonca i pravidiel, ktoré sa v týchto skupinách zdieľajú. Nebezpečným ho robí aj to, že dnes sa už dá bežne kúpiť na darknete ako ‚služba‘,“ varuje Jaroslav Ďurovka riaditeľ Národného centra kybernetickej bezpečnosti.

Nie sme výnimka

Ján Doboš z Národného centra kybernetickej bezpečnosti potvrdzuje rastúci trend aj na Slovensku: „Ransomvér sa týka každého z nás, bez ohľadu na veľkosť organizácie, a bývajú zasiahnuté aj fyzické osoby.“ V minulom roku bolo evidovaných viacero ransomvérových útokov, pričom iba minimum z nich bolo medializovaných, či už ide o súkromný sektor alebo verejnú správu.

Útoky boli detegované, keď sa prejavili náhodné výpadky služieb či spomalenie počítačov, pričom boli objavené súbory s podozrivými prílohami. V niektorých prípadoch to bolo cielené „bombardovanie“ a zneužitie prístupových údajov, v iných zanedbanie kyberbezpečnostnej hygieny.

Slabé miesta

Analytický tím Coveware upozorňuje, že malé a stredné firmy predstavujú takmer dve tretiny obetí ransomvéru. V minulom kvartáli zasiahol ransomvér globálne najmä organizácie s počtom zamestnancov od sto do tisíc. Tesne za nimi nasledujú ešte menšie firmy či inštitúcie od desať do sto zamestnancov.

Menej robustné bezpečnostné systémy v malých firmách sú totiž lákavým cieľom. Investície do najmodernejších bezpečnostných riešení sú privysoké a rovnako nepravdepodobný je špecializovaný interný tím. Okrem toho, menšie organizácie často platia výkupné, aby rýchlo obnovili systémy a údaje.

Ako sa to začne

V malých podnikov sa útočníci pokúšajú získať neoprávnený prístup k počítaču alebo sieťovému zariadeniu. Pri útoku hrubou silou využívajú automatizované nástroje alebo softvér, ktorý generuje a testuje veľké množstvo používateľských mien a hesiel za krátky čas. Skúšajú, skúšajú, až trafia.

Aktéri útokov na stredné až veľké podniky využívajú zraniteľností, a čoraz sofistikovanejšie techniky sociálneho inžinierstva. Sem patria aj útoky SIM Swap, keď útočník zmanipuluje operátora, aby preniesol číslo obete na jeho SIM kartu.

Miliarda výkupného

Spoločnosť Chainalysis, ktorá sa špecializuje na sledovanie pohybu kryptomien, hlási rekord – miliarda dolárov v minulom roku ako výkupné pri ransomvéri. Je to takmer dvojnásobný medziročný rast.

Report Coveware však uvádza, že čoraz viac organizácií odmieta platiť výkupné. V štvrtom štvrťroku 2023 zaplatila výkupné menej ako tretina obetí (29 percent), pričom pred piatimi rokmi to bolo 85 percent platiacich.

Organizácie tvrdia, že sú už lepšie pripravené a neveria útočníkom, že nezverejnia ukradnuté údaje. V niektorých štátoch je už dokonca zaplatenie výkupného nelegálne.

S čím počítať

Ak rastie objem zaplateného výkupného a zároveň obete odmietajú platiť, má to dva hlavné dôvody – útočníci pýtajú vyššie výkupné a súčasne pribúda aj útokov.

Frekvencia a závažnosť útokov závisia od rôznych faktorov ako geografická poloha či príslušnosť k sektoru. Vzhľadom na citlivosť a hodnotu údajov sú však atraktívnymi cieľmi zdravotníctvo, financie a energetika.

Samotný zločinecký biznis je stále lepšie organizovaný, drajvovaný umelou inteligenciou či podporovaný štátnou mocou. Odborníci sa zhodujú, že rozsah aj sila ransomvéru budú rásť.

Hlásiť alebo utajiť

Kybernetický útok nie je hanba. A ak ide o ransomvérový incident, na jeho zvládnutie je nevyhnutný špeciálny proces a spôsob manipulácie s infikovanými zariadeniami. Preto sa v tomto prípade odporúča koordinácia so špecializovaným tímom.

Pre prevádzkovateľov základných služieb je hlásenie závažného incidentu štátnej autorite povinné. Ján Doboš však odporúča aj dobrovoľné hlásenia, keď môže NCKB aktívne pomôcť skúsenosťami či vydať varovanie pre príslušný segment. V konečnom dôsledku, o samotnom incidente môže komunikovať výlučne postihnutý subjekt a spolupracujúci profesionáli sú viazaní mlčanlivosťou.

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

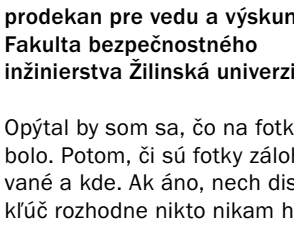
Že by pomohlo zaplatiť a do pár minút bude všetko naspäť bez akýchkoľvek následkov? Neverím, že by to niekto myslel vážne. Takže: Neplatiť, neplatiť a ešte raz neplatiť. No a, samozrejme, čo najskôr inštalovať kvalitnú ochranu.

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.

Cesta od detekcie založenej na signatúrach k pokročilej behaviorálnej analýze odráža príbeh vývoja kybernetickej bezpečnosti. SNÍMKA: DREAMSTIME

Je to symfónia stratégií

TECHNOLÓGIE

S vývojom kybernetických hrozieb sa vyvíjajú aj metódy boja proti nim. V boji proti ransomvéru je dôležitá synergia medzi rôznymi technológiami a prístupmi.

Príbeh bezpečnosti

Prvú líniu obrany pred malvérom spočiatku poskytovali metódy založené na signatúrach, ktoré predstavujú spôsob overenia identity softvéru alebo jeho častí. Tieto metódy porovnávali známe odtlačky malvéru so súbormi, aby v nich identifikovali hrozby.

Obmedzenia tohto prístupu sa však ukázali, keď kyberzločinci vyvinuli polymorfný a metamorfný malvér, ktorý dokáže zmeniť svoj kód tak, aby sa vyhol detekcii.

Tu nastupujú heuristická analýza a analýza správania. Tieto metodiky analyzujú správanie programov s cieľom identifikovať podozrivé aktivity naznačujúce škodlivý softvér, ako sú neoprávnené zmeny systému alebo neobvyklá sieťová aktivita. Posun od statického prístupu založeného na signatúrach k dynamickej stratégii zameranej na správanie znamenal významný pokrok v možnostiach detekcie malvéru.

Nové generácie

Antivírusové systémy novej generácie (Next Generation Antivirus - NGAV) vznikli ako reakcia na vyvíjajúce sa prostredie hrozieb s využitím kombinácie tradičných techník a pokročilých technológií, ako je strojové učenie a analýza správania.

Riešenia NGAV presahujú rámec jednoduchého porovnávania signatúr a ponúkajú komplexnú ochranu pred širokou škálou kybernetických hrozieb vrátane útokov nultého dňa a sofistikovaných kampaní.

Systémy rozšírenej detekcie a reakcie (Extended Detection and Response - XDR) dopĺňajú antivírusové systémy novej generácie a ponúkajú zastrešujúci rámec, ktorý integruje údaje z rôznych bezpečnostných vrstiev – koncových bodov, sietí, serverov či cloudových služieb.

Holistický prístup XDR poskytuje možnosti diferencovanejšie chápať modely hrozieb a uľahčuje odhaľovanie komplexných, viacstupňových útokov. Koreluje rôznorodé dáta a odhaľuje celý rozsah útoku, čím umožňuje koordinovanejšiu a účinnejšiu reakciu.

Líder obrany

Ransomvér so svojím ničivým vplyvom a obrovskou prispôsobivosťou zostáva jednou z najvýznamnejších hrozieb v oblasti kybernetickej bezpečnosti. Umelá inteligencia tu stojí na čele obrany a ponúka inovatívne nástroje na predvídanie, odhaľovanie a reakciu na ransomvérové útoky skôr, ako stihnú napáchať škody.

Systémy poháňané umelou inteligenciou analyzujú rozsiahle súbory údajov s cieľom identifikovať podprahové, čiže nepatrné vzorce a anomálie, ktoré môžu uniknúť ľudským analytikom alebo tradičnému softvéru. To umožňuje preventívne zasiahnuť proti potenciálnym ransomvérovým hrozbám.

Navyše, schopnosť umelej inteligencie učiť sa umožňuje, aby sa časom prispôsobila novým taktikám ransomvéru.

Na všetkých frontoch

Boj proti škodlivému kódu sa nevedie na jednom fronte, ale prostredníctvom hlboko prepojenej siete technológií a stratégií. Synergia medzi NGAV, XDR a AI stelesňuje moderný prístup ku kybernetickej bezpečnosti - jednotný obranný mechanizmus, ktorý využíva silné stránky jednotlivých komponentov na vytvorenie robustnej a prispôsobivej bezpečnostnej stratégie.

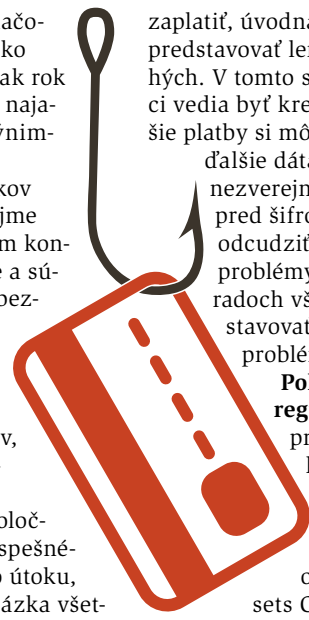
Základom integrovaného riešenia je schopnosť AI analyzovať obrovské množstvo údajov v nevídanom rozsahu a rýchlosti, pričom identifikuje vzorce a anomálie, ktoré môžu naznačovať kybernetickú hrozbu. V kombinácii so systémom XDR, ktorý konsoliduje údaje z viacerých bezpečnostných vrstiev, je výsledkom komplexný a diferencovaný systém detekcie a reakcie na hrozby.

Algoritmy strojového učenia dokážu identifikovať typické vzorce správania ransomvéru, akými sú rýchle šifrovanie súborov alebo pokusy o pripojenie k známym serverom na riadenie a kontrolu ransomvéru. V kombinácii s komplexnou viditeľnosťou XDR v celej sieti táto schopnosť zabezpečuje, že aj tie najsofistikovanejšie ransomvérové útoky možno identifikovať a neutralizovať v ich ranom štádiu.

Július Selecký,
senior technický špecialista ESET,
odborný asistent
na Fakulte managementu UK

PORADŇA

Platiť či neplatiť? Zopár faktov aj bez bez Hamleta



Hoci rok 2022 naznačoval, že ransomvér ako útok je na ústupe, tak rok 2023 nám dal jasne najavo, že išlo skôr o výnimku ako o pravidlo.

Pokles počtu útokov v roku 2022 bol zrejme spôsobený vojnovým konfliktom na Ukrajine a súhlasím s tvrdením bezpečnostných expertov. „Ten, kto očakával dlhodobý trend ústupu ransomvérových útokov, nepochopil ich základnú motiváciu."

Ak sa však už spoločnosť stala obeťou úspešného ransomvérového útoku, na rad prichádza otázka všetkých otázok: Platiť či neplatiť?

Keďže pre niektoré spoločnosti môže byť otázka výkupného priam hamletovskou dilemou, myslím, že pred jej vyriešením je vhodné zvážiť nasledujúce fakty.

Znehodnotené dáta. V niektorých prípadoch ransomvérových útokov bola väčšina súborov nad 64 kilobitov znehodnotených. Iný prieskum uvádza, že len polovica tých, čo zaplatili, sa dostala k všetkým svojim dátam. Útočníci nie sú práve najdôslednejší, čo sa týka dátovej manipulácie. Prečo by aj boli? Ich motivácia je iná.

Motivácia útočníkov dostáť záväzkom je značne limitovaná. Prečo by to aj robili, keď už dostali zaplatené? Ako aj vyplýva z teórie hier, pokiaľ ide o „hru" s konečným počtom opakovaní – čo je v tomto prípade jedno, protistrana je silno motivovaná správať sa nečestne, aby pri tejto jednokolovej výmene maximalizovala svoj úžitok. O samotnej cnosti útočníkov, verím, nemusíme ani len diskutovať.

Stávate sa potenciálnym cieľom ďalších útokov. Informácia o tom, ktoré spoločnosti sú ochotné zaplatiť a ktoré nie, sa šíri aj v komunitných kruhoch týchto dnes už organizovaných skupín. Takouto platbou by ste sa poľahky mohli nominovať do neželanej ligy. A čo viac, pravdepodobne by útočníci neskončili pri jednej transakcii.

Viacnásobné vydieranie. Ak útočníci zistia, že ste ochotní zaplatiť, úvodná platba môže predstavovať len jednu z mnohých. V tomto smere útočníci vedia byť kreatívni a ďalšie platby si môžu pýtať za ďalšie dáta či za to, že ich nezverejnia, keďže ich pred šifrovaním mohli odcudziť. Ekonomické problémy vo vlastných radoch však môžu predstavovať len časť vašich problémov.

Pokuty zo strany regulátorov. Úrad pre kontrolu zahraničných aktív (U.S. Treasury Department's Office of Foreign Assets Control – OFAC) vydal jasné stanovisko, keď pridal ransomvér ako druh kybernetickej hrozby na sankčný zoznam. V rámci tohto zoznamu tak môže pokutovať subjekty, ktoré útočníkov podporujú. Hoci je toto rozhodnutie zamerané na subjekty pod jurisdikciou USA, pri dnešnom globalizovanom svete je nutné zvážiť aj túto skutočnosť.

Samotné výkupné pritom nepredstavuje jediné náklady, ktoré spoločnosť musí vynaložiť na čo najefektívnejšie zotavenie sa z útoku. Napríklad americký gigant MGM vo svojej finančnej správe vyčíslil škody spôsobené ransomvérovým útokom na 100 miliónov dolárov. Výkupné, samozrejme, odmietol zaplatiť a jeho výška nie je známa.

Ak je v kybernetickej bezpečnosti zrejmé, že prevencia je oveľa lacnejšia ako neskoršie riešenie incidentu, tak v prípade ransomvérových útokov toto pravidlo platí dvojnásobne.

Tak ako v každom prípade potenciálneho kybernetického útoku je vhodné zastaviť ho čo najskôr spolu so sprievodnými vektormi. Preto nie je na škodu si spraviť proaktívne cvičenie odolnosti proti ransomvérovým útokom napríklad s pomocou modelu Cyber Kill Chain od spoločnosti Lockheed Martin, ktorý definuje a opisuje jednotlivé fázy útoku.

Michal Srnec
CISO Aliter Technologies

RIEŠENIA

Počet gangov rastie, zlepšujú sa techniky, tak nečakajte v kúte

Aby sme vedeli predchádzať ransomvérovým útokom či reagovať na ne, pozrime sa na podstatu tejto formy zločinu.

Zoberme do úvahy počet aktívnych organizovaných kriminálnych skupín orientujúcich sa na tieto typy útokov. Za jediný rok – ten minulý – sa počet ransomvérových gangov zvýšil o tretinu a skončil na čísle 47.

Taktiky a techniky, ktoré využívajú, majú vždy za cieľ finančné obohatenie. Platba je v kryptomenách a vydieranie naberá na intenzite.

Máme problém

Ransomvér už nie je len o škodlivom kóde, ktorý obmedzuje prístup k počítaču či šifruje dôležité súbory.

Dnes už nie je výnimkou, že kým vyskočí na obrazovke pomyselná správa „úctivej žiadosti o výkupné", útočník sa dávno dostal k citlivým informáciám a rôznym osobným údajom. Toto je jeho najsilnejšia páka na získanie výkupného.

Vydieračské metódy sú s každým útokom košatejšie a agresívnejšie. Kriminálnici zneužívajú odcudzenú identitu na iné kriminálne skutky či blokujú a diskreditujú obchodné operácie tým, že zverejnia firemné údaje. A čím väčšia obeť, tým útok trvá dlhšie a zanecháva väčšie škody.

Tri cesty do pekla

Spôsobov, ako sa môže útočník dostať do počítača, je niekoľko.

Najčastejšie sú to techniky sociálneho inžinierstva, najmä phishingu. Obeť sa „nachytá" inštaláciou škodlivého softvéru bezhlavým kliknutím na ponúknutý produkt či službu, ktorá údajne vyrieši jeho problém. Alebo sa nechá nalákať na rôzne výhody s vidinou zisku na sociálnych sieťach.

Druhou, a veľmi masívnou formou, je využitie dávno ukradnutých prístupov k službám vzdialenej plochy na zariadeniach, ktoré sa dnes masívne povaľujú na darkwebe.

Treťou je zneužívanie softvérových zraniteľností v rôznych typoch IoT zariadení pripojených do internetu, ako napríklad inteligentné termostaty, kamery, osvetľovacie systémy a podobne.

Niečo ako votrelec

Keď sa už útočník dostane do počítača, hrá sa o čas. A toho dnes majú útočníci čoraz viac, dokonca viac, ako potrebujú.

Kriminálne skupiny sústreďujúce sa na „väčšie ryby" využijú napadnutý počítač, aby sa dostali do rozsiahlych infraštruktúr veľkých firiem a verejnej správy. Tam sa pohybujú mesiace či roky často nepozorovane a dokážu napáchať rozsiahle škody.

Úniky citlivých dát, získavanie prístupov do informačných systémov, maskovanie svojej prítomnosti a mazanie stôp, zanechávanie zadných dvierok pre ďalšie útoky, poškodzovanie záloh pre obnovu. Proste čokoľvek, čo môže napomôcť finančnému obohateniu.

Testujte, skúšajte

Za posledné roky sa určite zlepšilo povedomie o kybernetických hrozbách vo firmách a verejnej správe, ale ransomvérové gangy nespia na vavrínoch.

Organizácie všetkých veľkostí a vo všetkých odvetviach by sa preto mali zamerať najmä na testovanie pripravenosti na incidenty. Povinnou jazdou by malo byť v súčasnosti testovanie odolnosti simulovaním ransomvérových útokov.

Prínosom testov je najmä vyhodnotenie ochrany a formy obrany koncových zariadení, počítačovej siete a štruktúry záloh až po obnovu po incidente.

Zároveň sa takto identifikujú slabé miesta v IT infraštruktúre organizácií či absencia technických a procesných opatrení. Tu dávam dôraz predovšetkým na detekciu a obnovu systémov zo záloh po incidente.

My všetci

Ako bežní používatelia môžeme každý deň pomáhať neustálou aktualizáciou operačných systémov a aplikácií na našich osobných zariadeniach. Bežnou rutinou by mala byť kvalita hesiel a záloh a obmedzenie bezhlavého zdieľania osobných informácií na sociálnych sieťach.

A ak by ste mali mať stále na pamäti jednu a nekonečne dobrú radu – neskočte na phishingový háčik, ktorý na nás číha v každom kúte digitálneho priestoru.

Roman Čupka,
hlavný konzultant Progress,
CSO Istrosec

Ransomvérový útok si môžeme predstaviť ako misiu útočníka dostať sa nepozorovane z Bratislavy do Košíc.

Ukradnuté auto v Bratislave nám reprezentuje napadnutý prvý počítač. Košice sú pomyselný server, kde sa dôležité dáta zašifrujú. Cesty, diaľnice a železnica sú počítačovou sieťou. Ransomvér je preto taký úspešný, lebo dnes je ťažké ochrániť proti krádeži každé auto v Bratislave a útočník môže cestou do Košíc niekoľkokrát zmeniť formu cestovania.

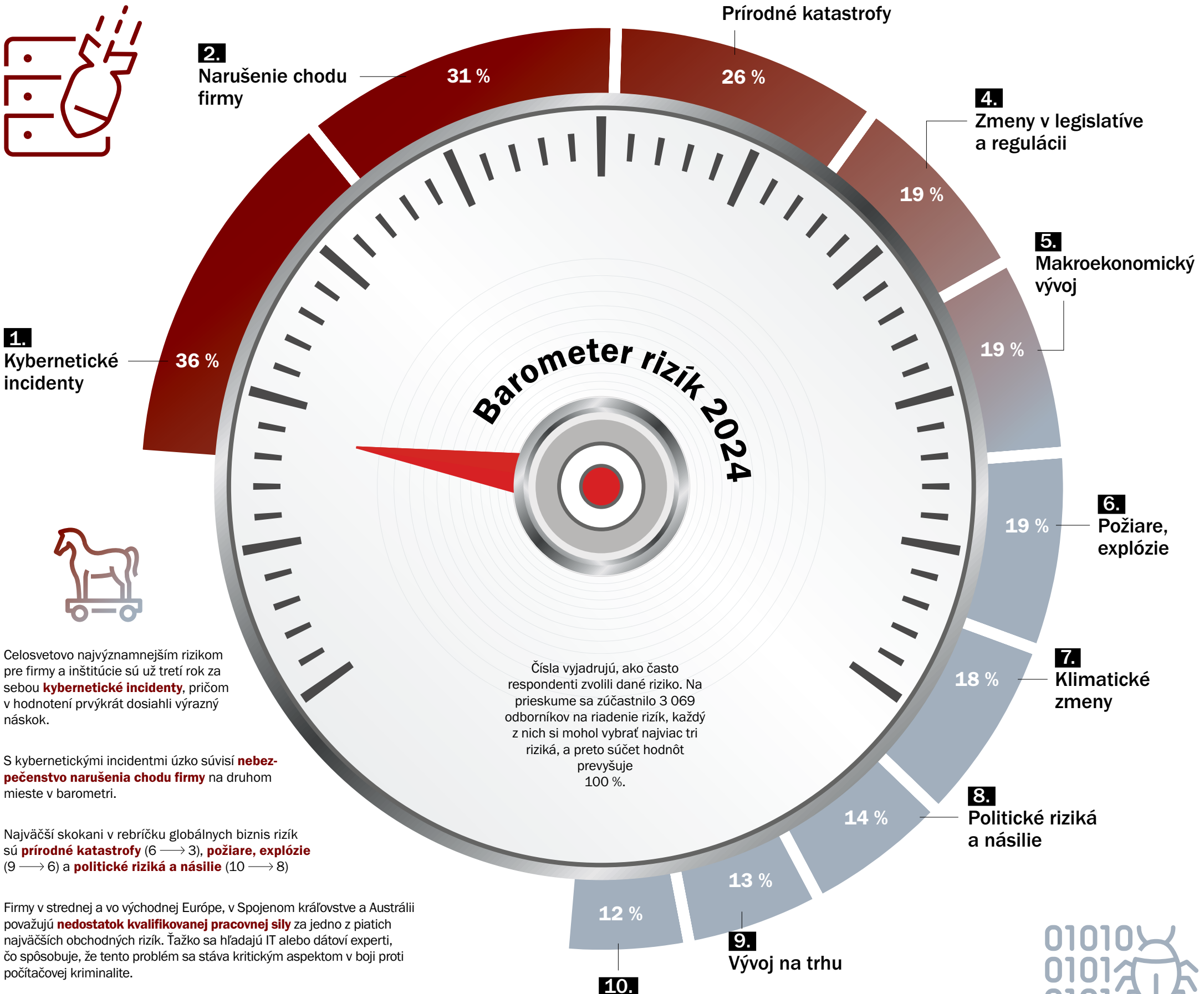
Útočník na tejto ceste využíva každú príležitosť nedostatočného kamerového systému v uliciach. V každom cestovnom prostriedku po jeho opustení zanechá bombu či sledovacie zariadenie. Pohyb a aktivity mení v závislosti od toho, čo potrebuje urobiť a ako sa maskovať. Takže útočník súčasne zametá stopy a ešte si so sebou berie všetko cenné, čo objaví. No a keď dorazí do Košíc, už sme prehrali. Už je neskoro.

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

Čo trápi firmy vo svete a kde číhajú najväčšie riziká

Závažné kybernetické hrozby podľa hodnotenia respondentov

Narušenie ochrany údajov	59 %
Útoky na kritickú infraštruktúru a fyzický majetok	53 %
Ransomvérové útoky	53 %



Čísla vyjadrujú, ako často respondenti zvolili dané riziko. Na prieskume sa zúčastnilo 3 069 odborníkov na riadenie rizík, každý z nich si mohol vybrať najviac tri riziká, a preto súčet hodnôt prevyšuje 100 %.

Celosvetovo najvýznamnejším rizikom pre firmy a inštitúcie sú už tretí rok za sebou **kybernetické incidenty**, pričom v hodnotení prvýkrát dosiahli výrazný náskok.

S kybernetickými incidentmi úzko súvisí **nebezpečenstvo narušenia chodu firmy** na druhom mieste v barometri.

Najväčší skokani v rebríčku globálnych biznis rizík sú **prírodné katastrofy** (6 ⟶ 3), **požiare, explózie** (9 ⟶ 6) a **politické riziká a násilie** (10 ⟶ 8)

Firmy v strednej a vo východnej Európe, v Spojenom kráľovstve a Austrálii považujú **nedostatok kvalifikovanej pracovnej sily** za jedno z piatich najväčších obchodných rizík. Ťažko sa hľadajú IT alebo dátoví experti, čo spôsobuje, že tento problém sa stáva kritickým aspektom v boji proti počítačovej kriminalite.

Znepokojivý nárast strát

Po dvoch rokoch vysokej, ale stabilnej straty došlo v roku 2023 k nárastu strát spojených s ransomvérom a vydieraním.

Aktéri hrozieb sa čoraz viac zameriavajú na IT a fyzické dodávateľské reťazce, iniciujú masové kybernetické útoky a hľadajú nové spôsoby, ako získať výkupné od veľkých aj malých firiem.

Ktoré organizácie sa najviac obávajú narušenia svojho chodu

Odvetvia a oblasti, kde organizácie najviac znepokojuje ich odolnosť v rámci kybernetickej bezpečnosti

životné prostredie

sociálne veci

vládne organizácie

predaj spotrebného tovaru

finančné služby

zdravotná starostlivosť

telekomunikácie

Kľúčom k úspechu je včasná detekcia

Význam zručností a nástrojov včasného odhaľovania útokov a reakcie neustále rastie.

Ak spoločnosti nemajú účinné nástroje včasnej detekcie, dôsledkom môžu byť dlhšie neplánované odstávky, zvýšené náklady a väčší vplyv na zákazníkov, výnosy a reputáciu

Schopnosť včasnej detekcie a účinnej reakcie bude kľúčom k zmierneniu vplyvu kybernetických útokov

Zdroj: Štúdiu Allianz Risk Barometer každoročne zostavuje Allianz Commercial - korporátna poisťovňa skupiny Allianz - spolu s ďalšími subjektmi Allianz.
Zohľadňuje názory viac ako tritisíc odborníkov na riadenie rizík v deväťdesiatich dvoch krajinách a teritóriách vrátane generálnych riaditeľov, manažérov rizík, maklérov a odborníkov na poistenie