Otázne už nie je – za koľko peňazí, ale ako

Kybernetická kriminalita predstavuje masívny a agresívny ekosystém špecializovaných dodávateľov. FOTO: SHUTTERSTOCK

TREND

Technologický pokrok, robustnosť infraštruktúry a dostupnosť značného výpočtového výkonu vytvárajú nevídané príležitosti pre sofistikované a masové útoky.

Fenoménom súčasnosti je fakt, že útočníkom aj obeťou môže byť doslova ktokoľvek a kdekoľvek na svete.

Argumenty, že moje podnikanie alebo moje údaje nemôžu byť pre nikoho zaujímavé, prípadne moja konkurencia sa na nič také nezmôže, už dnes neobstoja. Útoky vykonávajú často roboty, ktoré hľadajú ľubovoľnú slabinu v ochrane prostredia alebo systému, a identita obete je pre ne až sekundárna.

Bariéry v nás

Hlavným „problémom“ celej kybernetickej bezpečnosti je fakt, že ide o komplexnú oblasť, ktorá sa zároveň veľmi dynamicky vyvíja. Preto si málokto vie predstaviť, čo to znamená mať vo firme alebo v organizácii vhodne zavedené prvky kybernetickej ochrany a mať túto oblasť spoľahlivo zabezpečenú.

S tým sú, samozrejme, spojené otázky: „Aké drahé je ochrániť našu firmu pred kybernetickými útokmi? Je potrebné zamestnávať odborníkov a zaobstarať najnovšie technológie?“

Prístupy môžu byť rôzne, no aj tu platí isté ratio, aby nás výsledná investícia do tejto oblasti nemusela nutne bolieť. Ale hlavne, aby bola efektívna, škálovateľná a vhodná pre konkrétny typ spoločnosti.

Alchýmia tohto storočia

Bez prvotnej analýzy využívaných nástrojov, komunikačných kanálov a celkovej infraštruktúry spoločnosti je akákoľvek implementácia skôr špekulatívna alchýmia s veľmi neurčitým výsledkom.

Odborníci na základe takejto analýzy konkrétneho prostredia vedia odporučiť vhodné štandardizované postupy a riešenia, ktoré chránia to najcennejšie a najkritickejšie, čím spoločnosť disponuje, a zároveň predikujú a eliminujú budúce ohrozenia.

Služby na vzostupe

Zaujímavou alternatívou posledných rokov je, po vzore cloudových technológií, zabezpečenie ochrany kybernetického priestoru formou služby. V takom prípade nie je potrebné vo firme zamestnávať, manažovať a neustále školiť vlastných pracovníkov, ani neuvážene nakupovať softvér a nové hardvérové prvky ochrany.

Kybernetickú bezpečnosť zastrešujú odborníci z externej firmy, ktorí majú skúsenosti so stovkami bezpečnostných incidentov a situácií. Navyše, keďže ich služby sú zdieľané viacerými klientmi, ekonomická výhodnosť takéhoto riešenia v čase „normálnej“ prevádzky je nepopierateľná. Zároveň pri existujúcom incidente je zásah skúsených odborníkov omnoho efektívnejší ako v prípade fixného zamestnanca.

> Útoky vykonávajú často roboty, ktoré hľadajú ľubovoľnú slabinu v ochrane prostredia alebo systému, a identita obete je pre ne až sekundárna.
>
> **Tomáš Orieščik,** CTO Aliter Technologies

Kauza hasiči

Pri téme kyberbezpečnosti sa často vynára aj otázka prístupu k nej. Investovať naslepo do prevencie alebo si počkať na prvý väčší problém a zaplatiť až za „hasičov“?

Odpoveď nechám na vás, ale na uľahčenie rozhodovania uvediem zaujímavý príklad – nedávne nabúranie do jedného zahraničného e-shopu. Incident na prvý pohľad ochromil produkčný web. Došlo k výpadku objednávok, klesli tržby.

Zamrzí, no všetko sa podarilo relatívne rýchlo obnoviť. Až neskôr zistili, že útok znehodnotil dáta už v existujúcich objednávkach a informáciách o platbách, čím znemožnil korektné dodanie tovaru. Okrem vlastných technických problémov musela spoločnosť čeliť strate osobných údajov klientov, prácne kontaktovať každého dotknutého zákazníka, riešiť krízové PR a, samozrejme, implementovať opatrenia, ktoré už mohli byť dávno zavedené, ak by včas riešili prevenciu.

Rukojemníci nevedomosti

Z uvedeného je jasné, že aj relatívne jednoduché útoky dokážu zastaviť podnikanie v jedinej sekunde a spôsobiť problémy na nasledujúce obdobie. Riziku pritom vystavujeme nielen seba a svoju firmu, no ohrozujeme aj svojich zákazníkov.

Ten, kto to myslí dnes s podnikaním seriózne, musí mať popri štandardných výdavkoch v rozpočtoch zahrnutú aj položku na zabezpečenie svojej kybernetickej zraniteľnosti.

PORADENSTVO

Pán riaditeľ, vyhovárať sa nedá donekonečna

Na budovanie kybernetickej bezpečnosti by sa dalo minúť neuveriteľné množstvo času a peňazí, ale tie nemáte.

Veľa firiem potrebuje zvýšiť svoju schopnosť odolať útoku kyberútočníka. No uvedomujete si, čo to znamená? Hovoríte, že budovanie odolnosti je finančne náročné? Áno aj nie. Je to určite náročné na čas a odhodlanie.

Bez financií to asi tiež nepôjde, ale začať sa dá rozhodne aj bez nich. Je tu pár domácich úloh a stoja „len“ čas a chuť sa do nich pustiť. A neverte ani tomu, že túto domácu úlohu za vás niekto urobí, aj keď vám to ponúka.

Najdôležitejšou je inventarizácia vašich aktív a procesov. Aktívum je niečo ako váš poklad. A keď neviete, čo chcete chrániť, dodávateľ vám to nepovie.

Ak sa však firma ocitne na pokraji svojej schopnosti niekam sa posunúť v budovaní kybernetickej ochrany, začne zvažovať, že si niekoho prizve, kto jej bude vedieť pomôcť.

Práve v tejto chvíli budete potrebovať určiť, čo je nevyhnutné obstarať a za akú cenu. Tu je niekoľko nutných podmienok a rád, ako uspieť a nestratiť veľa peňazí.

Aj týmito pravidlami viete zredukovať prepotrebné peniaze a navyše ich významne rozložiť v čase.

Budujte odolnosť, nie dokumentáciu

Nezačínajte obstaraním dokumentácie. Tá vás pred útokom nezachráni a ak nemáte postavenú kybernetickú obranu, nie je čo dokumentovať. Aj napriek tomu, že je veľa dodávateľov, ktorí by to ochotne urobili, dokumentácia má byť obrazom vášho stavu organizácie a nie iba víziou.

To je ako chcieť podrobný prevádzkový manuál k super autu, ktoré ešte neexistuje. Ak by ho niekto napísal, počas konštruovania auta ho musí tisíckrát upraviť a nakoniec bude pramálo podobný tomu na začiatku.

Cena nie je všetko

Nestanovujte ako jediné kritérium na výber odborných služieb cenu. Nie ste taký bohatý, aby ste si vedeli kupovať predražené neefektívne riešenia.

To je, ako keby ste si vyberali jedlo len na základe ceny. Je jedno, ako to chutí, hlavne, že je to najlacnejšie. To naozaj nechcete. Už to len vysvetliť kolegom pri obstarávaní.

Začnite s otázkou PREČO

Veľmi jasne identifikujte cieľ implementovaného opatrenia kybernetickej bezpečnosti. Aj vy, aj dodávateľ musíte rozumieť tomu, čo potrebujete dosiahnuť.

Často sa stretávam napríklad s tým, že firmy obstarávajú SIEM – technológiu bezpečnostného monitoringu siete, ale nevedia, čo a prečo budú monitorovať. A najmä vôbec neplánujú budovať schopnosť s touto informáciou niečo následne urobiť. Cieľom nie je mať SIEM, ale vedieť zasiahnuť proti útoku.

Dodávateľ pracuje pre nás a nie my pre dodávateľa

Nenechávajte dodávateľa bez vašej podpory. Ak dodávateľ pracuje sám a odovzdá vám „len“ výsledky svojej práce, nemusia napĺňať vaše ciele. Navyše si potrebujete výsledky dodávateľa osvojiť, prijať ich a zaradiť do svojho prostredia.

Často sa stáva, že práca dodávateľa zostane nedotknutá, bez pochopenia výsledkov a izolovaná od ostatného prostredia vo firme. V tom prípade prichádzate práve o tie peniaze, ktoré tak potrebujete ušetriť.

David Dvořák, audítor kybernetickej bezpečnosti

V organizácii každého typu za kybernetickú bezpečnosť zodpovedá štatutár. FOTO: SHUTTERSTOCK

PRAX

Nevieme povedať, koľko vás to bude stáť, kým nevieme, čo máte

Riadenie informačnej bezpečnosti je dôležitá súčasť strategického plánu každej organizácie. Zosúladí úroveň informačnej bezpečnosti s aktivitami, legislatívnymi požiadavkami a očakávaniami trhu.

Nadýchnite sa

Budovanie bezpečnosti v organizáciách často okrem nedostatku ľudských zdrojov stroskotá na financiách.

Preto je nutné sa na tento proces dôkladne pripraviť. Nezačínať kúpou bezpečnostného softvéru, ale správnou analýzou. Predídete takým banalitám, ako je vynaloženie väčších prostriedkov na ochranu, ako sú samotné dáta, ktoré chránite.

Vyvarujte sa omylu

Často sa stretávame so situáciou, keď zákazník žije v domnienke, že pomocou šifrovania, viacfaktorovej autentizácii či XDR nastolí vo firme „bezpečnosť“. A pritom kroky, ako napríklad riešenia na ochranu koncových bodov, by sa mali vykonávať až následne.

Budovanie bezpečnosti je komplexný proces, ktorý si vyžaduje skúsenosti v prvom rade na strane poskytovateľa bezpečnostných služieb.

Premyslite si to

Bezpečnosť každej organizácie sa začína tromi cieľmi: dôvernosť, dostupnosť a integrita. Ide o akýsi priemyselný štandard. Potrebujete zabezpečiť, aby sa k citlivým informáciám dostali iba oprávnené osoby, a teda aby tieto dáta neboli prezradené neoprávneným subjektom.

Zároveň je nutné, aby ste sa k vlastným dátam dostali vtedy, keď to potrebujete. V neposlednom rade je dôležité, aby jednotlivé informácie mohli meniť len oprávnení ľudia či prostriedky. V preklade to znamená, že informácie neboli narušené a sú úplné.

Hodnoťte s odstupom

Od dostupnosti, dôvernosti a integrity závisí kvalita poskytovaných služieb a schopnosť organizácie efektívne dosahovať ciele. Aby ste tento stav dosiahli, potrebujeme poznať, čo má význam vo vašej firme chrániť. Reč je o aktívach.

Môže ísť o procesy, ľudí, softvér, komponenty či know-how. K tomu, aby sme poznali aktíva, nám dopomôže analýza rizík.

Použite nástroje

Analýza rizík je základný nástroj systému riadenia informačnej bezpečnosti, pomocou ktorého dokážeme vyhodnotiť priority bezpečnosti v organizácii.

V prvej fáze identifikujeme a klasifikujeme aktíva a stanovíme požiadavky na bezpečnosť. Takto budeme vedieť, čo je pre vás najdôležitejšie.

V ďalšej fáze identifikujeme zraniteľnosti a posudzujeme hrozby, ktoré na tieto aktíva pôsobia. Potrebujeme pochopiť, kto vás chce či môže napadnúť a prečo a ako to môže uskutočniť. Špecialista následne určí dosah zneužitia zraniteľnosti danou hrozbou. Až následne po týchto úkonoch dokážeme určiť hodnotu, respektíve závažnosť jednotlivých rizík.

Výstupom analýzy bude katalóg aktív so zoznamom identifikovaných rizík s opisom a so závažnosťou.

Poznajte sa

Cieľom analýzy je zistiť, čo je pre firmu alebo inštitúciu dôležité a cenné, aké riziko sú ochotné akceptovať a čo už nie je možné akceptovať vzhľadom na ich ciele. Definujeme takto v organizácii chuť riskovať.

Analýza rizík sa nevykonáva iba z dôvodu ochrany produktov či služieb, ale aj z dôvodov identifikácie potrieb v oblasti informačnej bezpečnosti. A v neposlednom rade práve kvôli optimalizácii nákladov v spoločnosti.

Rozhodnite sa

Až na základe výstupov z analýzy, s relevantnými dátami v rukách by sme mali pristúpiť k samotnej ochrane aktív napríklad pomocou šifrovania, viacfaktorovej autentizácie alebo komplexnej ochrany XDR, systémom na detekciu a reakciu.

Inak povedané, zabezpečujete svoje podnikanie na technologickej úrovni pomocou IT bezpečnostných riešení. A vtedy bude cena férová pre dodávateľa aj zákazníka.

Július Selecký, senior technický špecialista ESET, spol. s r. o., odborný asistent, Fakulta managementu UK