HN obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

PIATOK – NEDEĽA
15. – 17. DECEMBRA 2023

Partneri špeciálnej prílohy:
ALISON
ALITER TECHNOLOGIES

Dáte im dôveru, odplatou je útok

TÉMA

Prídu nenápadne zadnými vrátkami a čakajú. Ale úder je masívny, vyčerpávajúci a nikdy neviete, či sa už skončil. Tak by sa dal opísať útok cez dodávateľský reťazec.

Profesionálna dôvera firiem pri spolupráci nie je postačujúci faktor pri budovaní kybernetickej odolnosti. FOTO: DREAMSTIME

Ešte pred tromi rokmi sa útokmi na dodávateľský reťazec zaoberali iba profesionáli v kyberbezpečnosti. Potom prišla kauza SolarWinds a médiá a aj my sme sa naučili, čo je to „supply chain attack".

Škodlivý kód sa infiltruje do softvéru, hardvéru alebo poskytovanej služby a kyberútoky zasahujú obete cez dodávateľa.

Úder pod pás

Keďže útok prichádza prostredníctvom dôveryhodného kanála alebo dodávateľskej služby, štandardné bezpečnostné mechanizmy sú proti takému typu útokov často bezmocné.

V softvérovej firme SolarWinds útočníci infiltrovali škodlivú funkcionalitu typu backdoor do softvéru Orion. Napadnuté aktualizácie si inštalovali zákazníci a nevedomky umožnili útočníkom získať neoprávnený prístup do svojich sietí. Obeťami sa stali tisícky organizácií vrátane vládnych agentúr a korporácií. Kyberbezpečnostný špecialista Jozef Bálint to považuje za míľnik, ktorý poukázal na to, aké vážne dosahy môže mať takýto typ útoku.

Slovenský príbeh

V prvej polovici roku 2023 médiá publikovali informáciu, že významná slovenská IT firma sa stala terčom ransomvérového útoku. Manažéri kybernetickej bezpečnosti v desiatkach spoločností a inštitúcií si po prečítaní uvedomili, že sú ich zákazníkmi a sú v ohrození. Ich údaje už možno majú útočníci.

V tej chvíli sa pre nich začali preteky s časom: Čo z uniknutých dát nám môže ublížiť? Sieťová dokumentácia? Zdrojové kódy? Prístupové údaje pre dodávateľa do našej siete? Takže – deaktivovať prístupy, pomeniť heslá, varovať zamestnancov pred blížiacou sa vlnou cieleného phishingu. Na všetko mali pár dní. Možno hodín.

Napadnutá spoločnosť napokon výpalné nezaplatila a dáta sa stali verejne dostupnými. Všetkým teda zostáva dúfať, že sa všetko zaplátalo včas.

Pravda je horšia

Celý príbeh, ako ho stručne opísal Milan Pikula z Národného centra kybernetickej bezpečnosti SK-CERT, má však ďalší rozmer. Klasikou bol ešte donedávna pokročilý útočník. Ten, čo s vidinou konečného cieľa identifikuje a napadne jeho dodávateľov. To evokuje mimoriadne hackerské zručnosti a takmer magickú schopnosť nepozorovane zasadiť do existujúceho softvéru zadné vrátka.

„Vybočme z mainstreamu. Útočníkom zneužijúcim dodávateľský reťazec sa odteraz môže stať absolútne každý, kto si vie stiahnuť pár súborov zo stránky ransomvérového gangu," varuje Milan Pikula.

Deravý softvér

Na kompromitovanie IT infraštruktúry a informačných systémov sa útočníci totiž snažia zneužiť najmä diery v softvérových nástrojoch, ktoré sa vo veľkom hojne využívajú. Roman Čupka, odborník v kybernetickej bezpečnosti, poukazuje na predpoveď, že do dvoch rokov sa stane obeťou zneužitia softvérových zraniteľností 45 percent organizácií vo svete. Je to trojnásobne viac ako v roku 2021.

Za týmto hrozivým trendom je rastúce využívanie open-source nástrojov, ktoré zo svojej povahy umožňujú upravovať kód komukoľvek. Tento ekosystém v súčasnosti obsahuje trojnásobne viac „zlomyseľných balíkov" ako vlani.

Tlak na výkon

Globálne používané komerčné softvérové nástroje obsahujú zraniteľnosti, ktoré vznikajú pri nedostatočnom otestovaní programátorského kódu či laxnosťou vývojárov. A je úplne jedno, či ide o diery v nástrojoch na správu hesiel, v prenose citlivých dát alebo operačných systémoch.

> Útoky na dodávateľský reťazec majú kaskádový efekt, zasahujú nielen dodávateľov a ich klientov, ale aj spotrebiteľov či pacientov.
>
> **Jozef Bálint**, kyberbezpečnostný špecialista

Podľa Roman Čupku však platí priama úmera a pravidlo, že čím kritickejší systém, robustnejšia inštalovaná báza a priamy prístup „do internetu", tým slastnejšie lákadlo pre útočníkov a väčšia pravdepodobnosť vzniku incidentu.

Ďalšie esá v rukáve

Nadšenci a profesionálne kriminálne skupiny tvoria čoraz sofistikovanejší škodlivý kód aj pomocou nástrojov umelej inteligencie. Preto ho je aj ťažšie identifikovať a odlíšiť napríklad od legitímnej aktualizácie či iných bezpečných častí kódu.

Tretia slabina kyberodolnosti spočíva v samotnej povahe súčasného obchodného modelu organizácií. Podniky sa čoraz viac technologicky prepájajú a vytvárajú s partnermi a dodávateľmi siete, pričom obchodnú dôveru prenášajú aj do kybernetickej bezpečnosti.

Roman Čupka tu upozorňuje napríklad na zanedbávanie šifrovania pri výmene citlivých dát alebo nedostatočnú pozornosť v bezpečnosti autorizovaných aplikácií, ktoré využívajú partneri v dodávateľsko-odberateľskom reťazci. Spolupracujúce organizácie si potrebujú dôverovať – a práve na zneužitie dôvery cielia útočníci.

Aktualizačný moment

Po viac ako roku sa európske inštitúcie zhodli na znení Nariadenia o kyberodolnosti. V praxi bude predstavovať právny rámec, ktorý opisuje požiadavky na kybernetickú bezpečnosť hardvérových a softvérových produktov uvádzaných na trh EÚ.

Riaditeľ odboru certifikácie KCCKB Ivan Kopáčik tým poukazuje na povinnosť výrobcov brať kyberbezpečnosť zodpovedne počas celého životného cyklu produktov. „Platí to pre všetok hardvér a softvér, od detských monitorov, inteligentných hodiniek a počítačových hier až po firewally a smerovače. Samozrejme, produkty s rôznymi úrovňami rizika budú mať rôzne bezpečnostné požiadavky."

Nariadenie priamo súvisí aj s rastúcou vlnou útokov zameraných na dodávateľské reťazce. Očakáva sa, že vďaka nariadeniu klesnú škody v dôsledku bezpečnostných incidentov v Únii každoročne o vyše 180 miliárd eur.

Nie sme výnimkou

Úspešné útoky na dodávateľský reťazec eviduje SK-CERT aj na Slovensku. „Prípady, ktoré sme pozorovali, sú prácou pokročilých skupín a konečným cieľom je štát," hovorí Milan Pikula. Apeluje preto na dodávateľov štátu, aby posilnili kybernetickú bezpečnosť. Špecialista Jozef Bálint z Alison Slovakia zas upozorňuje na kaskádový efekt útokov. Zasahujú nielen dodávateľov a ich klientov, ale aj spotrebiteľov či pacientov. Preto sa aj malá firma môže ľahko stať obeťou a kľúčovým prvkom v reťazci. Na zmiernenie rizík je, samozrejme, nevyhnutná ostražitosť, dôkladné hodnotenia rizík a dodržiavanie bezpečnostných opatrení na rôznych miestach dodávateľského reťazca. Vyberajte si primárne dodávateľov, ktorí disponujú bezpečnostnými certifikáciami a dodržiavajú štandardy, akými sú ISO certifikácie alebo špecifické odvetvové normy.

PREČÍTAJTE SI V PRÍLOHE

Desatoro, ako si overiť bezpečnosť dodávateľa

Kritické obavy bez rozdielu, pre veľké podniky aj malé firmy

Riziká reťazovej reakcie

Anketa: Kľúčový faktor kyberbezpečnosti 2024

Spoločnosti podieľajúce sa na obsahu špeciálnej prílohy

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti
auditori.it
CHECK POINT
eset
Progress
SOITRON
SK CERT NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 15. – 17. DECEMBRA 2023

Už si nevieme bez nich predstaviť svet

ANALÝZA

Info-komunikačné a prevádzkové technológie predstavujú bytostne dôležitú oporu pre firmy, inštitúcie a organizácie všetkých veľkostí a segmentov.

Info-komunikačné technológie (IKT) a prevádzkové technológie (OT) sú čoraz viac prepojené, čo zvyšuje ich komplexnosť a s tým aj riziko šírenia ohrození naprieč celým systémom. Preto sa akcentuje na dodávateľský reťazec IKT/OT ako na neoddeliteľný celok.

Nachádzajú sa tu kritické komponenty a softvér nevyhnutné pre bezpečné a spoľahlivé fungovanie dôležitých systémov a služieb. Akékoľvek zraniteľnosti alebo poruchy tu môžu mať významný dosah na celkovú bezpečnosť a funkčnosť systémov.

Dodávateľské reťazce IKT/OT sú zložité a často zahŕňajú mnoho rôznych subjektov. Udržiavanie integrity a autentickosti komponentov a softvéru je tu nevyhnutné na zabezpečenie, aby systémy neboli ohrozené sabotážou alebo neoprávnenými zásahmi.

Vzhľadom na to, že IKT/OT dodávateľské reťazce zahŕňajú mnoho rôznych dodávateľov, existuje riziko, že slabiny v bezpečnostných postupoch jedného dodávateľa môžu ohroziť celý systém. Preto si bezpečnostné riziká súvisiace s tretími stranami vyžadujú osobitnú pozornosť.

Významným faktorom je neustály vývoj v informačných aj prevádzkových technológiách. Ak chcú organizácie udržiavať krok s najnovšími technológiami, musia zároveň zabezpečiť, že ich dodávatelia dokážu reagovať zároveň s vývojom aj na nové hrozby a výzvy.

Riadenie rizík a zabezpečenie dodávateľského reťazca info-komunikačných a prevádzkových technológií sú kľúčové pre ochranu kritických infraštruktúr a služieb a zabezpečenie ich spoľahlivého a bezpečného fungovania.

Efektívne riadenie tohto dodávateľského reťazca pomáha organizáciám zároveň plniť regulačné požiadavky a štandardy týkajúce sa ochrany údajov, kybernetickej bezpečnosti a integrity systémov.

Cyklus riadenia rizík kybernetickej bezpečnosti dodávateľského reťazca info-komunikačných a prevádzkových technológií

- Poskytovať bezpečné produkty a služby
- Mať chránenú infraštruktúru
- Mať implementované bezpečné procesy
- Vytvoriť transparentnosť v IKT/OT dodávateľskom reťazci
- Merať kvalitu produktov a služieb

- Spravovať zraniteľnosti
- Poznať svoj majetok
- Rozumieť rizikám zraniteľností
- Monitorovať zraniteľnosti
- Opravovať zraniteľnosti
- Mať definovanú politiku údržby

- Rozumieť dodávateľskému reťazcu
- Identifikovať dodávateľov a poskytovateľov
- Rozumieť možným rizikám pre vlastnú organizáciu, ako aj pre koncových používateľov

- Riadenie IKT/OT dodávateľského reťazca
- Mať zavedené politiky a dohody
- Mať definované kyberbezpečnostné požiadavky
- Monitorovať výkonnosť dodávateľov a poskytovateľov služieb
- Riadiť zmeny

Riadenie rizík v dodávateľskom reťazci info-komunikačných a prevádzkových technológií

86 percent organizácií zaviedlo politiky kybernetickej bezpečnosti pre dodávateľský reťazec IKT a prevádzkových technológií.

14 percent opýtaných nemá schválené bezpečnostné politiky týkajúce sa tretích strán partnerov, predajcov, dodávateľov.

Čím väčšia je organizácia, tým je pravdepodobnejšie, že má zavedené príslušné politiky.

Pracovné pozície pre oblasť kyberbezpečnosti dodávateľského reťazca info-komunikačných a prevádzkových technológií

Väčšina opýtaných organizácií bez ohľadu na sektor nemá špecializované pracovné pozície pre kybernetickú bezpečnosť dodávateľského reťazca IKT/OT.

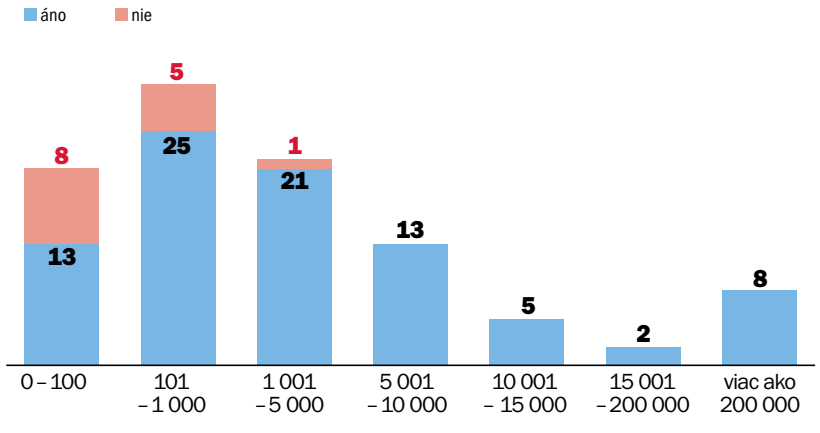
Najviac špecializovaných pracovných pozícií majú subjekty **v bankovníctve a zdravotníctve**.

Iba 24 percent oslovených organizácií má vyhradené roly a zodpovednosti pre kybernetickú bezpečnosť dodávateľského reťazca IKT/OT.

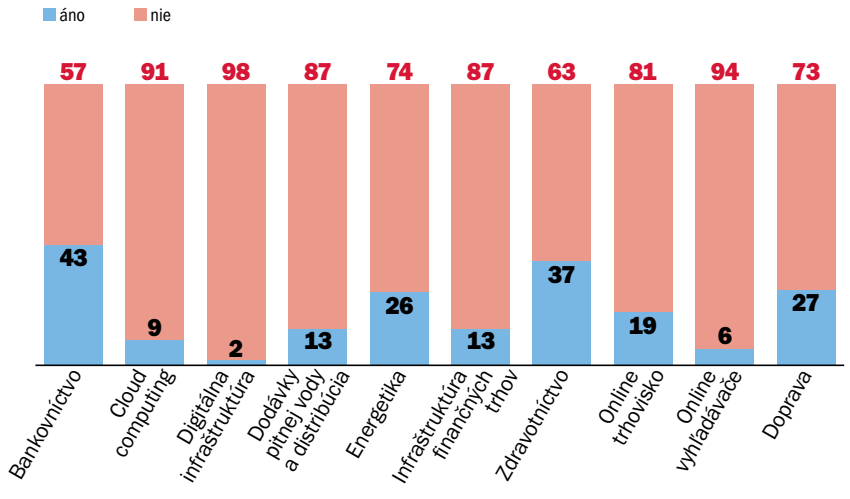
Stredne veľké organizácie majú prevažne vyčlenený rozpočet na bezpečnosť dodávateľského reťazca.

Prieskumnú štúdiu realizovala Agentúra EÚ pre kybernetickú bezpečnosť ENISA od apríla do júna 2022. Aby bolo zabezpečené adekvátne zastúpenie zo všetkých 27 členských štátov Únie, v každom členskom štáte bolo oslovených minimálne 40 organizácií zo segmentov bankovníctvo, digitálna infraštruktúra, dodávka a distribúcia pitnej vody, energetika, infraštruktúra finančného trhu, zdravotníctvo, dopravné sektory a poskytovatelia digitálnych služieb.

Schválené politiky riadenia rizík v dodávateľskom reťazci IKT/OT podľa veľkosti organizácie (údaje v percentách)



Pracovné pozície pre oblasť kyberbezpečnosti dodávateľského reťazca IKT/OT v sektoroch (údaje v percentách)



Zdroj: Správa Agentúry EÚ pre kybernetickú bezpečnosť ENISA o osvedčených postupoch kybernetickej bezpečnosti pre dodávateľský reťazec

Riziká reťazovej reakcie

FIRMY

Aj pri kybernetickej bezpečnosti platí, že každá organizácia je len taká silná ako jej najslabší článok. A ten sa môže nachádzať kdekoľvek v rámci jej dodávateľského reťazca.

Najviac kyberútokov smeruje na segmenty, ktoré spravujú citlivé údaje. FOTO: DREAMSTIME

Predstavte si, že niektorý z vašich subdodávateľov má k otázke kybernetickej bezpečnosti pasívny postoj. Ak aj vaša firma berie kybernetické hrozby vážne, môže stačiť slabé zabezpečenie obchodného partnera a jeho problém ohrozí aj vás.

Ako dôkazy môžu poslúžiť aj mediálne exponované prípady Kaseya či Solarwinds, kde útočníci cez ich kompromitáciu dokázali ohroziť aj celú bázu ich klientov.

Podobné útoky sa dejú vo všetkých oblastiach biznisu a výsledkom môže byť únik dát, ale aj pozastavenie výroby. Začiatkom minulého roka takýto scenár zažila Toyota, ktorá musela pozastaviť výrobu v štrnástich výrobných závodoch v Japonsku po tom, čo jej dodávateľa zasiahol kybernetický útok.

Nie je dôvod, aby to na Slovensku bolo inak. Aj u nás prakticky každá firma spolupracuje so subdodávateľmi. Podľa Slovak Business Agency tvoria malé a stredné podniky na Slovensku až 99,9-percentný podiel z celkového počtu podnikateľských subjektov.

Zaujímali ste sa však niekedy o bezpečnostné opatrenia zavedené u vašich, aj menších, dodávateľov? Myslíte si, že pristupujú k problematike kybernetickej bezpečnosti zodpovedne?

Až polovica firiem kybernetickú bezpečnosť nerieši

Národný bezpečnostný úrad spolu s Kompetenčným a certifikačným centrom kybernetickej bezpečnosti vykonali počas jari tohto roka prieskum zameraný na zistenie stavu kybernetickej bezpečnosti v malých a stredných podnikoch na Slovensku. Viac ako polovica respondentov v ňom uviedla, že ohrozenie kybernetickým útokom nepociťuje, a ani sa riadením kybernetických rizík nezaoberá.

Nie je preto prekvapujúce, že 60 percent týchto podnikov neposkytuje zamestnancom školenia v oblasti digitálnej bezpečnosti, ale zarazí, že takmer 75 percent (!) nevie pomenovať technickú alebo právnu normu, podľa ktorej opatrenia implementujú. Napríklad ISO27001 referencovalo 4,5 percenta a vyhlášku 362/2018 len jedno percento opýtaných.

Zdá sa, že ani legislatívne požiadavky nevytvárajú na podniky dostatočný tlak na to, aby zvyšovali svoju úroveň zabezpečenia. Prekvapivo to platí aj pri výrobných podnikoch, ktoré by sa už mohli zamýšľať nad dosahmi smernice NIS2.

Podniky kybernetické útoky nepriznávajú

V realite sú menšie podniky pre útočníkov ideálnym cieľom. Ako aj prieskum ukázal, o kybernetickej bezpečnosti nemajú dostatočné povedomie, nevenujú jej pozornosť, rozpočty či ľudské zdroje. A aj keď veľká väčšina firiem kybernetický útok verejne nepriznáva, neznamená to, že sa neudial.

V prieskume totiž až 40 percent stredných podnikov potvrdilo, že ich motiváciou na zvyšovanie úrovne zabezpečenia je práve poučenie z predchádzajúceho incidentu. Korešponduje to s prieskumom Eurobarometer 2022, kde 39 percent respondentov spomedzi slovenských podnikov uviedlo, že v uplynulom roku mali skúsenosť s kybernetickým zločinom. No paradoxne až 59 percent z nich takýto incident nikdy neohlási.

> Zdá sa, že ani legislatívne požiadavky nevytvárajú na podniky dostatočný tlak na to, aby zvyšovali svoju úroveň zabezpečenia.

Rozumiete svojmu dodávateľskému reťazcu?

Efektívne riadenie rizík v rámci dodávateľského reťazca môže byť veľmi komplexné a náročné, riadi sa však jednoduchými princípmi.

Svojmu dodávateľskému reťazcu musíte rozumieť. Mali by ste nielen vedieť, kto vaši dodávatelia a partneri sú, ale mať aj prehľad o tom, ako pristupujú k bezpečnosti a svojim subdodávateľom. To vám pomôže správne identifikovať riziká, ktoré pre vašu spoločnosť predstavujú, a následne zvoliť efektívne opatrenia pre ich mitigáciu.

Kľúčová je komunikácia – dodávatelia by mali poznať vaše požiadavky a očakávania. Zvážte zavedenie série nevyhnutných opatrení, ktoré budete v konkrétnych prípadoch vyžadovať, napríklad ak má mať dodávateľ prístup k vašim systémom alebo dátam.

Dodržiavanie týchto požiadaviek priebežne monitorujte a počítajte aj s ich zlyhaním – aby ste bezpečnostné incidenty, ktoré skôr či neskôr nastanú, dokázali identifikovať a reagovať na ne skôr, ako spôsobia katastrofu.

Netreba však zabudnúť na to, že správa rizík v dodávateľskom reťazci nie je jednorazový projekt, ale nikdy sa nekončiaci proces, ktorý si vyžaduje ostražitosť, prispôsobivosť a neustále zlepšovanie. V dnešnom rýchlo sa meniacom podnikateľskom prostredí je však rovnako dôležitý na prežitie a úspech vašej spoločnosti ako efektívna spolupráca samotná.

Silvia Strežová
void SOC, centrum kybernetickej bezpečnosti SOITRON

PORADŇA

Desatoro, ako si overiť bezpečnosť dodávateľa

Spoliehame sa čoraz viac na externých dodávateľov produktov a služieb, a to zdôrazňuje potrebu dôkladne posúdiť ich bezpečnosť. V desiatich krokoch zhrnieme kritériá a postupy, ako komplexne zhodnotiť bezpečnosť dodávateľa. Ide o informačnú a kybernetickú bezpečnosť, bezpečnosť prevádzky a riadenie tretích strán.

Štandardy bezpečnosti

Overte si, či dodávateľ dodržiava najnovšie štandardy kybernetickej bezpečnosti, napríklad ISO/IEC 27001:2022, alebo či sa na neho vzťahuje zákon o kybernetickej bezpečnosti.

Dáta a informácie

Váš dodávateľ by mal mať nastavenú klasifikáciu informácií. Následne aj opatrenia na ochranu spracúvaných, uložených aj posielaných informácií medzi ním, subdodávateľmi a vami ako odberateľom.

Uistite sa, že máte a vždy budete mať prístup k relevantným informáciám o bezpečnosti dodávateľa, ktoré sa týkajú vášho biznisu. Či už ide o správne nastavenú komunikačnú maticu, alebo o osobu, ktorá za dodávateľa zabezpečuje komunikáciu.

Riadenie rizík

Pýtajte sa na zavedené procesy riadenia rizík, poslednú analýzu rizík a najvyššie identifikované inherentné riziká u dodávateľa a zároveň aj na plán na zmiernenie rizík.

Personálna bezpečnosť

Váš dodávateľ by vás mal oboznámiť so svojimi postupmi vzdelávania v informačnej a kybernetickej bezpečnosti.

Dodávateľa by ste mali zaškoliť a pravidelne informovať o svojich špecifických bezpečnostných opatreniach a platnej prevádzkovej a bezpečnostnej dokumentácii.

Identifikujete, ktoré osoby dodávateľa budú zapojené do plnenia zmluvných záväzkov a v akej miere.

Preventívne opatrenia

Dodávateľ by vám mal poskytnúť informácie o zavedených organizačných, procesných a technologických opatreniach.

Detekčné opatrenia

Overte si, či má dodávateľ vytvorené mechanizmy identifikácie bezpečnostných incidentov a následne postupy rýchlej reakcie. Vhodné je, ak ich dodávateľ s vami vyskúša aj formou cvičenia.

Zmluvné záväzky

Zahrňte do zmlúv doložky týkajúce sa bezpečnosti a špecifikácie očakávaných štandardov a opatrení dodávateľa.

Trvajte na možnosti ukončiť zmluvný vzťah so všetkými náležitosťami ako zmazanie informácií a vrátenie aktív. Predchádzajte najmä stavu vendor lock.

Subdodávatelia

Ak má dodávateľ subdodávateľov, overte si, či aj tieto subjekty dodržiavajú rovnaké štandardy bezpečnosti.

Pravidelné audity

Požadujte pravidelné audity bezpečnosti a transparentnú správu o výsledkoch.

Poistenie

Dodávateľ by mal mať uzatvorené poistenie, ktoré chráni jeho aj vás v prípade kybernetických útokov alebo iných bezpečnostných incidentov.

Michal Ďorda,
audítor kybernetickej bezpečnosti, auditori.it

ŠTATISTIKA

Pre koho zúrivo bliká červená kontrolka?

V roku 2023 sú cieľom útokov na dodávateľské reťazce najčastejšie sektory finančných služieb, zdravotnej starostlivosti, technológií a telekomunikácií.

Disponujú hodnotnými údajmi a majú zložité dodávateľské reťazce, čo zvyšuje ich atraktivitu pre kybernetických zločincov.

Zdroj: Kroll Cyber Threat Intelligence

RIEŠENIA

Kritické obavy bez rozdielu, pre veľké podniky aj malé firmy

Útoky na dodávateľský reťazec zaznamenávajú raketový vzostup. Sú relevantné nielen pre obrovské nadnárodné spoločnosti so zložitou štruktúrou dodávateľov, ale aj pre malé a stredné podniky.

Základňa pre útoky

V typickom scenári získa útočník kompromitáciou dodávateľa prístup do informačných systémov zadávateľskej spoločnosti. Táto kompromitácia potom môže slúžiť ako základňa na ďalšie typy útokov, typicky s rozsiahlejšími dôsledkami.

Kým pri veľkých spoločnostiach je motivácia útočníkov zrejmá – kompromitáciou menšieho dodávateľa môže útočník dosiahnuť obrovský dosah v rámci veľkej spoločnosti, pri malých a stredných podnikoch to nemusí byť také zrejmé.

Nelimitovaná kreativita

Skryté riziko pre malé a stredné podniky predstavuje najmä fakt, že v rámci tohto typu útoku sa práve ony stávajú primárnym cieľom pre útočníkov. Malé firmy často nemajú dostatočne robustnú kybernetickú obranu, čo z nich robí pre útočníkov atraktívne ciele.

Verejná prezentácia spolupráce s veľkými spoločnosťami môže ešte zvýšiť ich atraktivitu pre kybernetických zločincov.

Ikonický príklad

Príklad, ktorým môžeme ilustrovať relevanciu, bol útok na americký gigant Target ešte v roku 2013. Vtedy sa táto obchodná sieť stala obeťou kybernetického prieniku, ktorý zapríčinilo zneužitie prístupových údajov dodávateľa klimatizačnej a vykurovacej techniky.

Útočníci získali prístup k citlivým údajom miliónov zákazníkov vrátane čísel kreditných a debetných kariet.

Princíp domino efektu vystihuje priebeh kybernetického incidentu. FOTO: DREAMSTIME

Útok spôsobil obrovské škody, nielen finančné, ale aj v oblasti dôvery zákazníkov a reputácie spoločnosti. Náklady na vyšetrenie incidentu, na opravy bezpečnostných systémov, právne náklady spojené so žalobami od zákazníkov a bánk a aj pokuty od regulačných orgánov sa ťahali roky. Odhadom v desiatkach miliónov až miliárd dolárov.

Softvér potrebuje každý

Útoky na dodávateľský reťazec môžu mať veľa foriem a využívať rôzne techniky. Významný rast však zaznamenali útoky na softvérový dodávateľský reťazec.

Obrovský tlak na rapídny vývoj softvérových riešení, používanie open-source knižníc či obrovská efektivita útoku len predznamenajú zrejmý nárast tohto konkrétneho typy útoku aj v budúcnosti.

Útočník si počká

Útočník môže implementovať zraniteľnosť do rozšírenej open-source knižnice, či dokonca celého repozitára a tak len s relatívne malým úsilím zaviesť zraniteľnosť k veľkému počtu klientov.

Navyše tento útok nemusí byť ani cielený a môže byť robený „plošne“. Útočníkovi potom stačí len čakať na využitie takejto knižnice.

Tomu typu útoku, samozrejme, hrá do karát aj kopírovanie riešení z portálov, ako je StackOverflow či používanie kódov priamo z Githubu.

Ako z toho von

Konať, samozrejme, musia tak malé, ako aj veľké spoločnosti: Pre tie väčšie podniky je nevyhnutné, aby implementovali opatrenia na monitorovanie a hodnotenie rizík spojených s tretími stranami a dôsledne vykonávali tzv. due deligence pri výbere dodávateľov.

Z technických opatrení môže pomôcť aj dodržiavanie „best practice“, ako je princíp minimálnych opatrení či prístup nulovej dôvery – zero trust.

Pre menšie podniky je však nutné vrátiť sa o krok späť. Tam treba začať s uvedomením, že práve kvôli ich spolupráci s veľkými firmami sa môžu stať obeťami kybernetického útoku. Nezostáva im nič iné, ako brať aj túto oblasť vážne – minimálne proaktívne monitorovať svoje aktíva a riadiť riziká.

Michal Srnec,
CISO Aliter Technologies

Kľúčový faktor kyberbezpečnosti 2024

ANKETA

Budúcnosť vzniká už dnes. Každý mesiac odpovedajú v ankete profesionáli, ktorí chránia náš kybernetický svet. Už dnes vidia to, čo nás bude ohrozovať aj zajtra. Požiadali sme ich, aby zvážili slovenské reálie, svoje profesionálne prostredie a praktický život.

Odpovedali na zásadnú otázku: Ktorý faktor bude najviac ovplyvňovať kybernetickú bezpečnosť v roku 2024?

Marián Illovský,
audítor kybernetickej bezpečnosti, auditori.it

Ľudský faktor.

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

Určite bude pretrvávať klasika, a to ransomvérové útoky. Ale na prvých husliach už hrá a bude hrať aj v roku 2024 určite umelá inteligencia, ktorá dokáže poradiť každému.

Jaroslav Ďurovka,
riaditeľ,
Národné centrum kybernetickej bezpečnosti SK-CERT

Hlavnou témou roku 2024 bude transpozícia a implementácia smernice NIS2. Jej zavedenie pomôže vo zvyšovaní odolnosti celého kybernetického priestoru Slovenska a Európskej únie voči bezpečnostným hrozbám. V aplikovanej bezpečnosti už dlhodobo sledujeme trend nárastu a sofistikovanosti ransom útokov, ktorých hlavným cieľom je vydieranie a finančný prospech. Predpokladáme postupné zvyšovanie kvality phishingových a iných kampaní založených na sociálnom inžinierstve. Pre potenciálne obete bude čoraz náročnejšie rozpoznať podvodnú komunikáciu od tej legitímnej.

Tomáš Hettych,
viceprezident,
ISACA

Jednoznačne pripravovaná novela zákona o kybernetickej bezpečnosti s ohľadom na smernicu NIS2. Ďalej to budú opakované výsledky auditov, ktoré už teraz ukazujú rastúci trend súladu a pripravenosti.

Andrej Žucha,
generálny riaditeľ,
ALISON Slovakia

Ten, čo aj doteraz. Človek za klávesnicou, jeho dôverčivosť a nepozornosť. Stačí jeden nevhodný klik a...

Roman Čupka,
hlavný konzultant,
Progress a CEO Synapsa Networks

V Spojených štátoch to budú aktuálne a pripravované prísnejšie bezpečnostné regulácie, v Európskej únii legislatívne zmeny, ktorých základom je aktuálna smernica NIS2 a pripravované nariadenie o kybernetickej odolnosti. Na Slovensku bude významným faktorom plán obnovy a flexibilita organizácií v čerpaní a alokovaní dostupných finančných prostriedkov. A ľudský faktor zostane aj naďalej tým najsilnejším a zároveň najslabším článkom v kybernetickej bezpečnosti.

Dominik Procházka,
riaditeľ odboru bezpečnosti,
AGEL SK

V roku 2024 bude rovnako ako dnes náročné zohnať šikovných ľudí na technické pozície, s čím je spojené riziko nesprávne zabezpečených prostredí, náchylnejších na útok. Z pohľadu útočníkov si myslím, že bude čoraz viac zneužívaná umelá inteligencia na generovanie dokonale vyzerajúcich podvodných kampaní a vysoká úroveň automatizácie pri hľadaní cieľov vo verejnom internete.

Zuzana Motúzová,
advokátka,
Motúzová & Lacko Advokátska kancelária

Jednoznačne to bude umelá inteligencia a súčasná geopolitická situácia. Ak sa tieto dva faktory spoja, máme pred sebou veľké bezpečnostné výzvy.

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

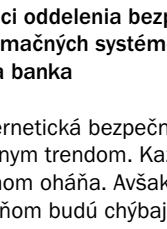
V roku 2024 sa určite nevyhneme nárastu množstva útokov sociálneho inžinierstva, ktoré budú čoraz dômyselnejšie aj vďaka generatívnym nástrojom umelej inteligencie. Preto by sme sa mali zamerať na bezpečnostné povedomie nielen v pracovnom, ale aj v súkromnom prostredí.

Marek Zeman,
vedúci oddelenia bezpečnosti informačných systémov, Tatra banka

Kybernetická bezpečnosť sa stala módnym trendom. Každý sa už pojmom oháňa. Avšak hlavným ťahúňom budú chýbajúci odborníci na kybernetickú bezpečnosť a nápady, ako ich získavať, respektíve zdieľať. Druhým ťahúňom bude boom okolo generatívnej umelej inteligencie. Čaká nás veľa prekvapení a firmy veľa sklamaní. Avšak tento boom pomôže čiastočne zaplniť chýbajúcu kapacitu na strane bezpečnostných expertov.

Július Selecký,
senior technický špecialista, ESET

Asi nikoho neprekvapím, keď poviem, že vďaka šíreniu dostupných nástrojov umelej inteligencie sa taktika útočníkov ešte viac posilní. V automobilovom sektore očakávam vzostup hackingu. Predpokladám, že do prezidentských volieb v USA výrazne zasiahnu deepfake videá.



Tomáš Zaťko,
CEO, etický hacker, Citadelo

Umelá inteligencia. A zatiaľ oveľa viac v marketingu ako v realite. To sa neskôr otočí.

Ján Andraško,
SOC manažér
Binary Confidence

Umelá inteligencia, tak na strane útočníkov, ako (dúfam) aj na strane obrancov.

Ján Grujbár,
generálny riaditeľ,
Aliter Technologies

Rok 2024 z hľadiska kyberbezpečnosti bude oveľa viac živý a dynamický a bude to rok plný technologických výziev a inovácií. Predstavte si, že všetky tie zariadenia okolo nás – od kávovarov až po továrenské stroje – budú súčasťou IoT, čo prináša kopu nových výziev v oblasti bezpečnosti. A to nie je všetko! Budeme sa musieť vyrovnať aj s „vychytralými“ AI systémami, ktoré nám budú pomáhať, ale zároveň aj skúšať naše obrany. A keď už hovoríme o obrane, tak práve ATP (Advanced Persistent Threats) – teda tieto zložité a dlhodobé útoky – budú ako čerešnička na torte. Navyše v roku 2024 nás čaká novelizovaný zákon o kybernetickej bezpečnosti. Bude to jazda!

Martin Lohnert,
riaditeľ centra kybernetickej bezpečnosti Void SOC, Soitron

Dovolil som si použiť „žolíka“ a opýtať sa nášho tímu SOC analytikov. Zhodli sa, že trendom roku 2024 bude všadeprítomná umelá inteligencia, ale kybernetickú bezpečnosť budú ešte stále viac ovplyvňovať práve ľudské faktory – dôverčivosť, nevedomosť, nezáujem.

Jaroslav Oster,
predseda správnej rady, Preventista.sk

Vidím tri dominantné faktory. Nárast množstva útokov postavených na manipulatívnych technikách, dynamický rast nástrojov umelej inteligencie používaných útočníkmi a zdĺhavé zvyšovanie bezpečnostného povedomia u všetkých sociálnych skupín.

Richard Kiškováč,
generálny riaditeľ,
Elkan

Kybernetickú bezpečnosť ovplyvňuje vždy viacero faktorov. Na rok 2024 bude dôležitým faktorom výkonnosť ekonomiky a dostupnosť zdrojov. Sú nevyhnutným predpokladom udržiavania adekvátnej úrovne kyberbezpečnosti. Samozrejme, k nástrojom sú potrební ľudia. Ich kvalita a dostupnosť je a bude dlhodobým otáznikom v privátnom aj vo verejnom sektore.

Alexander Varga,
informačný architekt, U. S. Steel Košice

Rok 2024 by mohol byť aspoň taký zaujímavý, ako bol ten posledný, keď pozorujeme masívny dopyt po IoT zariadeniach aj pripájanie prevádzkových technológií do infraštruktúr. Nastavenie správnej úrovne bezpečnosti s ohľadom na prevádzku bude znamenať konkurenčnú výhodu spoločností. Zásadné bude ešte podľa môjho názoru popri rozvoji umelej inteligencie neustále vzdelávanie odborníkov v oblasti kybernetickej bezpečnosti. To často rozhoduje, či budú bezpečnostné „hračky“ slúžiť, alebo niekde zapadať prachom.

Peter Dufek,
manažér kybernetickej bezpečnosti, Penta Hospitals

Najzávažnejším faktorom ovplyvňujúcim kybernetickú bezpečnosť bude boj o každého kvalifikovaného zamestnanca, expertov a špecialistov na kybernetickú bezpečnosť a čoraz komplikovanejšia geopolitická situácia vo svete.

Ivan Makatura,
generálny riaditeľ,
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Ľudia. Ich správanie a ich kvalifikácia. Tak ako doteraz. A možno ešte výraznejšie než doteraz.

Timea Tomčová,
manažérka útvaru IT architektúra a IT bezpečnosť, Union

Počas roku 2024 budú kybernetickú bezpečnosť a jej smerovanie formovať nepochybne vývoj a používanie umelej inteligencie, nové legislatívne požiadavky a veľké hrozby typu ransomvér.

Jakub Berthoty,
advokát,
Dagital Legal

Schopnosť organizácie vyrovnať sa s tým, že zmena kalendárneho roka na ňu nemá vplyv.

Diana Legdanová,
vedúca úseku bezpečnosti, Východoslovenská energetika Holding

Trojlístok v kyberbezpečnosti 2024 je prichádzajúca Smernica NIS2, dynamika rozvoja umelej inteligencie a vývoj geopolitickej situácie vo svete.

Tomáš Valenta,
riaditeľ,
Check Point Software Technologies na Slovensku

Mohol by som povedať, že peniaze či rozpočty, ale aj tak najvýznamnejší faktor kyberbezpečnosti bude zase len človek. Lebo iba ten môže urobiť správne rozhodnutia, vytvoriť budgety a posunúť kybernetickú bezpečnosť na ďalšiu úroveň. No a ešte taká „jednoduchá“ úloha nielen na rok 2024: nájsť toho človeka a nájsť ich veľa, lebo nedostatok ľudí v IT a bezpečnosti je alarmujúci.

Marián Trizuliak,
architekt kybernetickej bezpečnosti, Západoslovenská distribučná

Naďalej platí, že najslabším článkom bezpečnosti bol a v roku 2024 bude samotný človek. Z tohto pre mňa vyplývajú dva faktory – ľahostajnosť a egoizmus. Stále je nie malá množina ľudí úplne ľahostajná k nasadzovaniu opatrení, respektíve vnímaniu rizík ako takých. „Mne sa to nestane, veď máme antivírus a oddelenie bezpečnosti.“ Toto je mýtus, ktorý všetci v brandži poznáme a bojujeme s ním. A v predvianočnom čase nezabúdajme na „dôveryhodné internetové obchody“ s akciovými ponukami na všetko. Zámerne nespomínam finančné aspekty kybernetickej bezpečnosti – náklady boli, sú a budú potrebné aj naďalej.

Henrich Šnajder,
manažér IT bezpečnosti, Orange Slovensko

Jeden z kľúčových faktorov, ktoré budú ovplyvňovať náš kybernetický priestor, je implementácia opatrení v oblasti dodávateľských reťazcov IKT, ktoré zabezpečia väčšiu odolnosť voči kybernetickým hrozbám. Dodávateľské reťazce môžu predstavovať vysoké riziko aj pre dobre zabezpečené subjekty.