Varuhi kibernetske varnost

Mesec kibernetske varnosti

Glavne grožnje kibernetski varnosti in napovedi za leto 2025

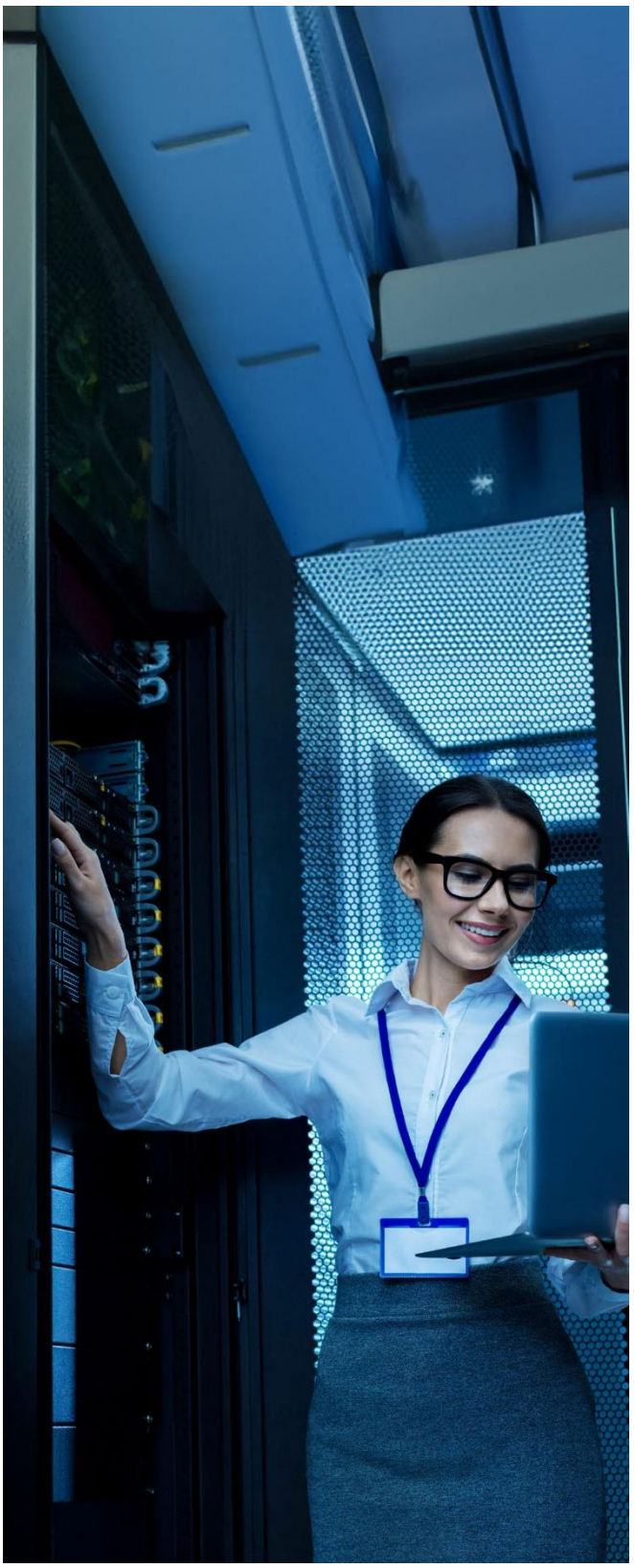
BDO

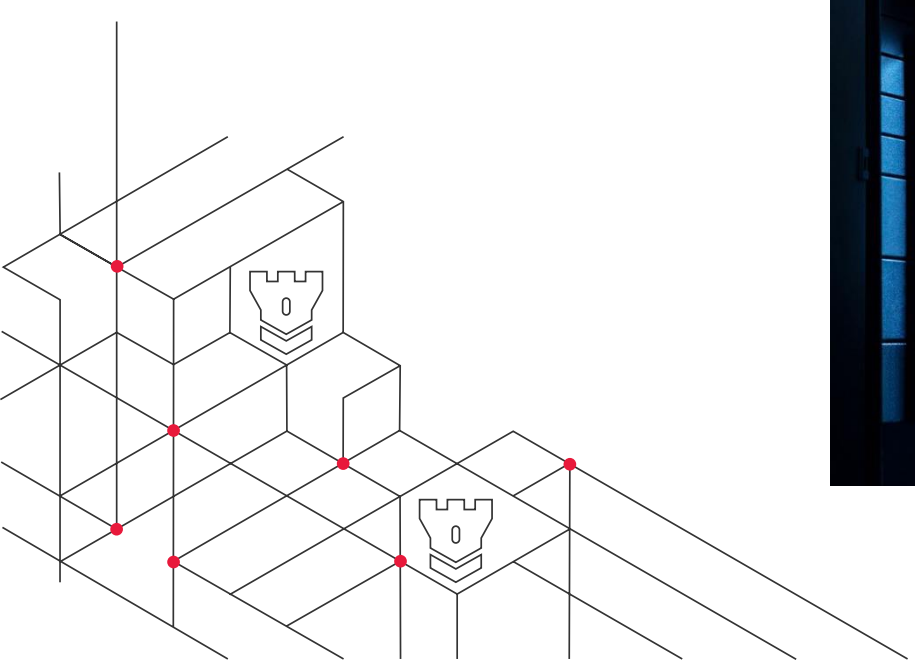
Glavne grožnje kibernetski varnosti in napovedi za leto 2025

Nova tehnologija omogoča analize ogromnega obsega podatkov, komunikacijo in operativno učinkovitost. Je pa to hkrati priložnost za kibernetske kriminalce – hekerje, ki postajajo vse bolj iznajdljivi. Posebej zaskrbljujoče je, da se v kibernetske napade vključuje tudi umetna inteligenca.

Če želite v tej digitalni tekmi ostati korak pred drugimi, morate sprejeti najsodobnejše ukrepe. Tako lahko npr. z uporabo varnostnih rešitev, ki temeljijo na generativni umetni inteligenci, drastično izboljšate delovanje skupin, ki skrbijo za varnost, povečate učinkovitost in zmanjšate tveganja. Varnostne tehnologije, ki temeljijo na generativni umetni inteligenci, lahko pomagajo pri odkrivanju tveganj višje prioritete in spodbujajo avtomatizirane postopke odzivanja.

Ključnega pomena je tudi razumevanje novih groženj, s katerimi se bodo organizacije soočale leta 2025. Ta članek obravnava največje grožnje in ključne strategije, ki vam bodo pomagale ohraniti zaščito.

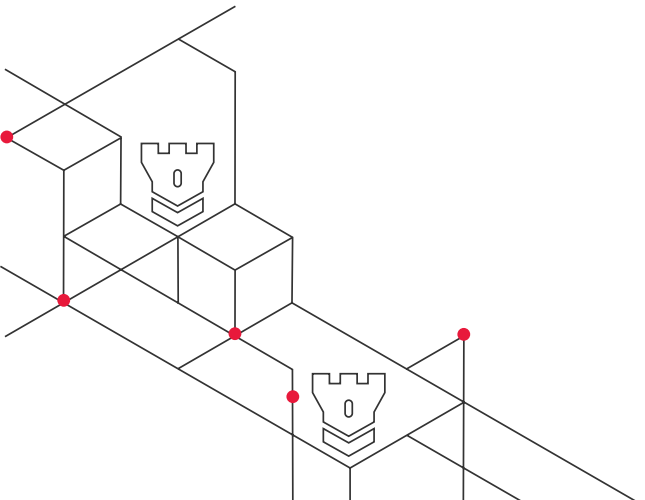




Naraščajoči stroški kibernetskih napadov in pomen obvladovanja tveganj na tem področju

Po podatkih IBM-ovega poročila o stroških vdora v sistem za leto 2024 so se stroški vdorov v letošnjem letu primerjavi s preteklim letom povečali za 10 %, kar je največje letno povečanje po pandemiji. Poleg tega se je v letu 2024 26 % več organizacij kot v preteklem letu, soočalo s hudim pomanjkanjem osebja na področju zagotavljanja kibernetske varnosti in je v povprečju zaznalo za 1,76 milijona USD višje stroške vdora kot organizacije, ki niso imele težav s pomanjkanjem osebja, ki skrbi za kibernetsko varnost. Vendar pa obstaja tudi nekaj dobrih novic: v poročilu je navedeno, da je bilo ugotovljenih približno 42 % vseh kršitev varnosti podatkov, kar je za 9 odstotnih točk več kot v preteklem letu. To povečanje gre pripisati večjim naložbam v zagotavljanje kibernetske varnosti.

Čeprav je trend obetaven, je še vedno veliko prostora za izboljšave na področju zagotavljanja kibernetske varnosti. Razvijajoče se okolje groženj, ki ga spodbujajo geopolitične napetosti in inovativne metode napadov, je vzrok za to da organizacije stalno razvijajo in testirajo varnostne mehanizme, ki jih imajo vzpostavljene za obvladovanje kibernetskih tveganj. Uporaba orodij umetne inteligence lahko osebju zagotovi dodaten čas, da se lahko osredotoči na nenehne izboljšave.



Kdo so glavni akterji kibernetskih groženj?

Vaša kibernetska varnost ni le skrb IT, morala bi biti temeljni vidik vaše poslovne strategije. Sposobnost krmarjenja po zapletenem spletu groženj kibernetske varnosti ni več stvar konkurenčne prednosti, temveč pravna in etična obveza. Sprejeti so bili strogi zakoni in predpisi, ki organizacijam nalagajo, da ostanejo pozorne in proaktivne pri varovanju svojih podatkov, da bi ohranile svojo integriteto, zaupanje in zasebnost svojih strank in partnerjev.
Za učinkovito zmanjševanje tveganj morajo organizacije do leta 2025 prepoznati in obravnavati naslednje grožnje:

Nacionalno-državni akterji

Gre za posebno državno telo znotraj nekaterih držav, ki imajo organizirano skupino hekerjev za napade ključnih ciljev drugih (neprijateljskih) držav. Gre za ene najbolj organiziranih in sposobnih skupin na področju izvajanja kibernetskih napadov. Ti namreč veliko vlagajo v kibernetske zmogljivosti, tako ofenzivne kot defenzivne, da bi pridobili geopolitične prednosti. Njihove dejavnosti pogosto narekujejo širše trende na področju kibernetske varnosti.

Ob trenutnih geopolitičnih napetostih v vzhodni Evropi in zahodnem Pacifiku bodo ti akterji še naprej določali nove trende na področju kibernetske varnosti.

Na ofenzivni strani države razvijajo platforme in orodja za kibernetske napade, ki so pogosto zelo občutljivi in tajni, namenjeni pa so prikriti uporabi ob izbranem času in na izbranem kraju. Včasih so ti sistemi objavljeni ali razkriti in jih namerno uporabljajo kriminalne združbe ali celo druge države.

Na obrambni strani vladne agencije, kot je Komisija za vrednostne papirje in borzo (SEC) v Združenih državah Amerike, zaostrujejo predpise o kibernetski varnosti za podjetja, delno kot odziv na prefinjene grožnje nekaterih držav.

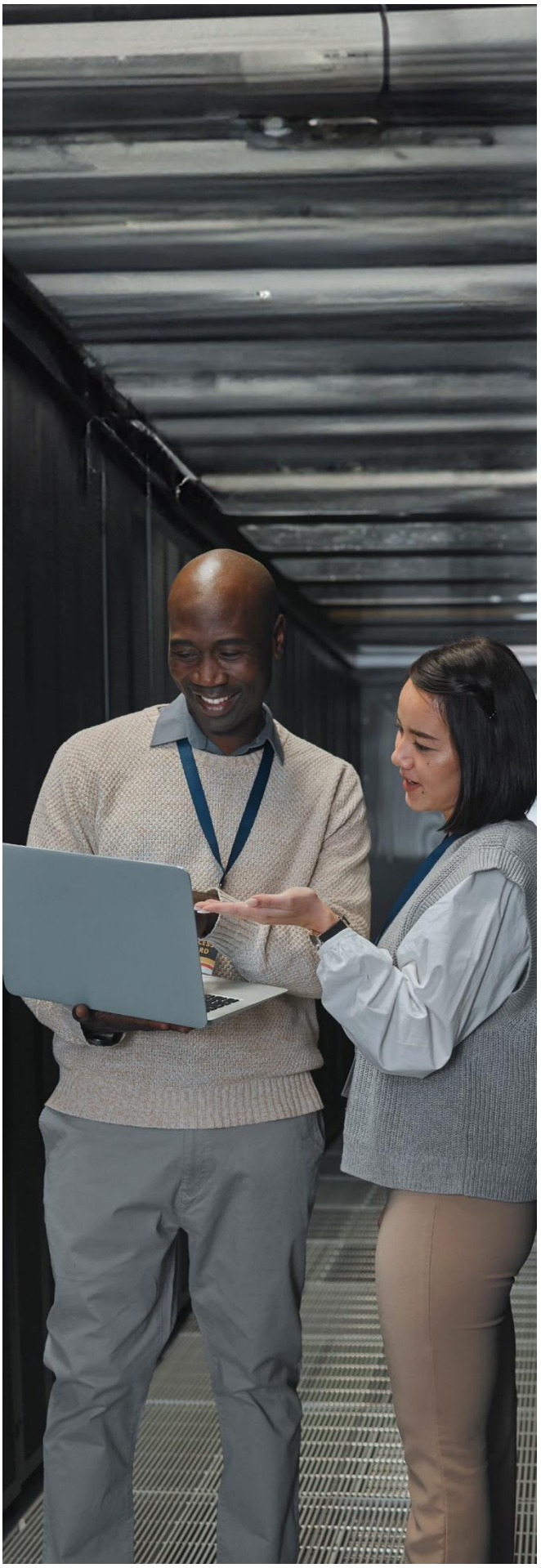
Kibernetski kriminalci

Skupine kibernetskih kriminalcev se pogosto osredotočajo na finančni dobiček in so različne, od prefinjenih skupin, ki včasih delujejo z določeno podporo države (kot posredniki), do manj organiziranih, vendar visoko usposobljenih skupin. Poleg tega, orodja, ki jih uporabljajo državni akterji, včasih namerno ali nenamerno pridejo v roke teh kriminalcev, kar še poveča tveganje.

Posamezni hekerji

Na drugi strani so posamezni hekerji in majhne skupine, ki jih pogosto imenujemo hekerski navdušenci. Njihovi motivi so različni, od aktivizma do finančnih koristi ali slave. Tehnologije, ki omogočajo hekanje, postajajo vse bolj dostopne prek platform, ki ponujajo "hekanje kot storitev", kar omogoča, da tudi manj izkušeni posamezniki predstavljajo precejšnje tveganje.

V današnjem povezanem svetu nobena organizacija ni popolnoma varna pred kibernetskimi grožnjami, zato morajo podjetja nujno razumeti spreminjajoče se okolje groženj. Ta ekosistem je zapletena mreža različnih akterjev, od katerih ima vsak edinstveno motivacijo in zmožnosti, kar predstavlja vrsto tveganj za finančno in operativno celovitost organizacij.



Katere so glavne kibernetske grožnje?

V današnjem medsebojno povezanem svetu nobena organizacija ni popolnoma varen pred kibernetskimi grožnjami, zaradi česar je nujno za podjetja, da razumejo razvijajoče se okolje groženj. Ta ekosistem je zapletena mreža različnih akterjev, od katerih ima vsak edinstveno motivacijo in zmožnosti, ki predstavljajo razpon tveganj za finančno in operativno integriteto organizacij.

Kibernetsko vohunjenje

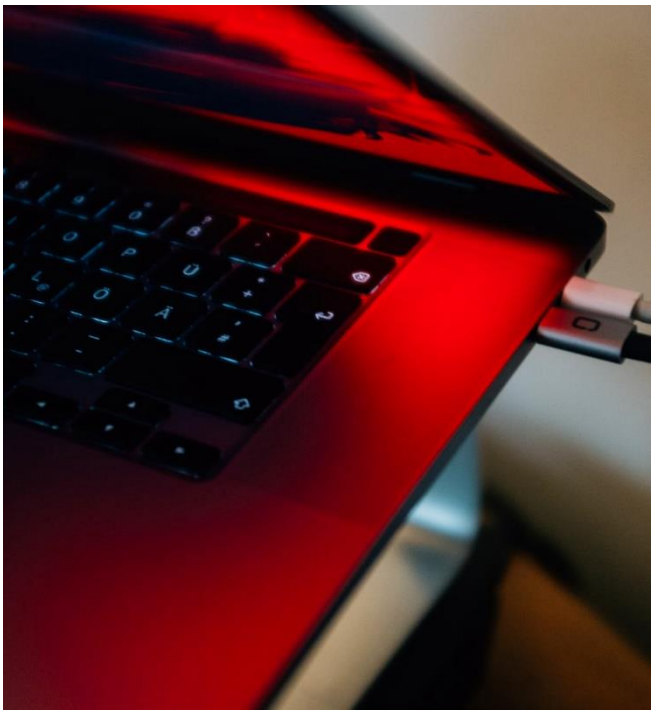
Ta prikrita grožnja vključuje nepooblaščen dostop do računalniških sistemov in omrežij z namenom zbiranja občutljivih informacij, kar lahko povzroči hude posledice. Te lahko segajo od uničenega ugleda organizacije ali izgube konkurenčne prednosti do ogrožene nacionalne varnosti. V tem kontekstu je razumevanje običajnih taktik kibernetskega vohunjenja ključnega pomena za izvajanje učinkovitih protiukrepov.

▷ Kompromitiranje poslovne e-pošte

Za napade s poslovno e-pošto je značilna zavajajoča preprostost, saj se v e-poštni komunikaciji izdajajo za zaupanja vrednega posameznika ali subjekt, da bi zaposlene, stranke ali potrošnike prepričali v razkritje občutljivih informacij ali izvedbo goljufivih finančnih transakcij. To lahko pogosto povzroči velike gospodarske izgube in škodo ugledu.

▷ Zloraba gesel

Hekerji uporabljajo ukradena uporabniška imena in gesla iz enega spletnega mesta za dostop do drugih računov, pri čemer izkoriščajo posameznike, ki uporabljajo ista gesla za prijavo na več platformah. Ta taktika temelji na ponovno uporabljenih geslih, zato je učinkovita metoda za ogrožanje računov in dostop do občutljivih informacij.



▷ Interne grožnje

Glede na nedavno Verizonovo poročilo povprečna zunanja grožnja ogrozi približno 200 milijonov zapisov, medtem ko so incidenti, v katere je vključen notranji akter, povzročili izpostavljenost 1 milijarde zapisov ali več. Gre za pomembno taktiko kibernetske grožnje, pri kateri posamezniki z odobrenim dostopom do sistemov in podatkov organizacije izkoriščajo svoj položaj. Ti posamezniki so lahko zaposleni, pogodbeniki ali poslovni partnerji.

▷ Napadi na dobavno verigo

Gre za napade pri katerih heker zlorabi ranljivost varnostnega sistema zunanjega dobavitelja, da pridobi dostop do omrežja druge organizacije. Tako lahko ogrozijo varnost celotne dobavne verige, kar lahko privede do vdora v podatke, ogrožanja sistemov ali drugih škodljivih posledic. Proaktivno zmanjševanje tveganja je bistvenega pomena za preprečevanje te večplastne in razvijajoče se grožnje.

Kibernetska sabotaža

Gre za namerna dejanja motenja digitalne infrastrukture z namenom ogroziti celovitost, zaupnost ali ugled ciljne organizacije. Razlogi za napad so lahko osebne narave ali konkurenčne. Ključno je razumeti, katere vrste napadov so najpogostejše in kako se pred njimi zaščitimo. Najpogosteje gre za naslednje vrste napadov:

▷ Izsiljevalska programska oprema (angl. Ransomware)

V poročilu Microsoft Digital Defence Report 2023 je navedeno, da so se organizacije v primerjavi s prejšnjim letom soočale s povečano stopnjo napadov izsiljevalske programske opreme, pri čemer se je število napadov izsiljevalske programske opreme, ki jih je upravljal človek, povečalo za več kot 200 % v primerjavi s preteklim letom. Za izsiljevalsko programsko opremo je značilno šifriranje ali včasih spreminjanje ključnih podatkov, da bi od ciljnih žrtev izsilili odkupnino. Kibernetski kriminalci vse bolj sodelujejo, si izmenjujejo orodja in taktike ter širijo mreže, da bi napadli organizacije vseh velikosti. Ti dejavniki so prispevali k vse pogostejšim in zahtevnejšim incidentom z izsiljevalsko programsko opremo, ki predstavljajo veliko tveganje za organizacije po vsem svetu.

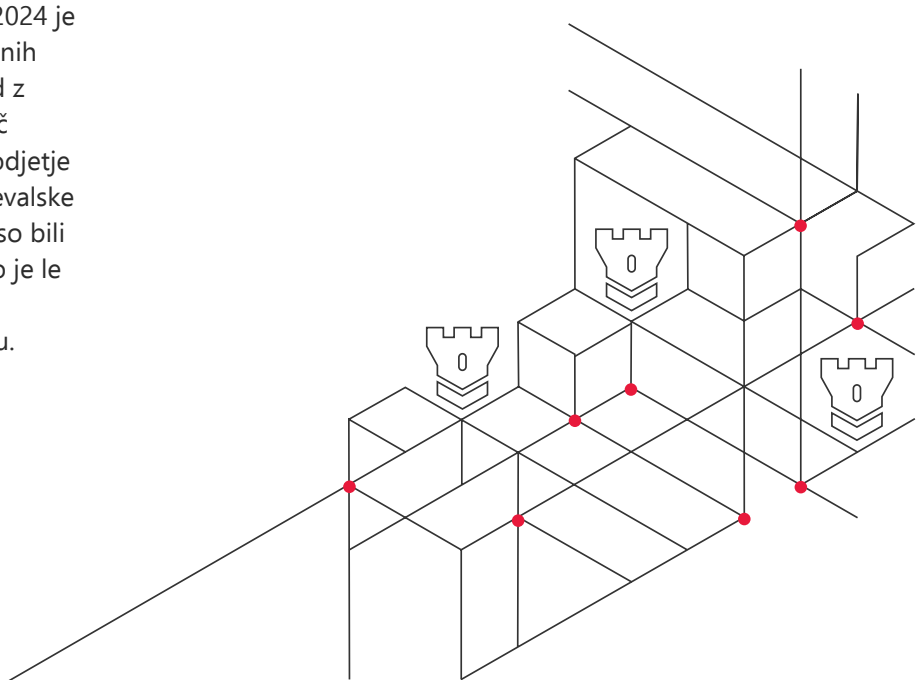
Oktobra 2023 je bila javna knjižnica v Torontu, največja kanadska knjižnična mreža, žrtev napada izsiljevalske programske opreme. Kibernetski kriminalci so šifrirali računalniške sisteme knjižnice in ukradli podatke zaposlenih, kar je povzročilo obsežne motnje pri izvajanju storitev. Maja 2024 je podjetje Ascension, enega največjih neprofitnih zdravstvenih sistemov v ZDA, prizadel napad z izsiljevalsko programsko opremo, ki je za več tednov prekinil delovanje. Februarja pa je podjetje Hyundai Motor Europe doživelo napad izsiljevalske programske opreme Black Basta, v katerem so bili ukradeni trije terabajti podatkov podjetja. To je le nekaj primerov incidentov, ki so pomembno vplivali na organizacije in ljudi po vsem svetu.

▷ Zavrnitev storitve

Cilj napadov z zavrnitvijo storitve (DoS) je onemogočiti dostopnost spletnih storitev ali spletnih mest tako, da se njihovi strežniki preplavijo s prometom in postanejo nedostopni za legitimne uporabnike. Pri tem se običajno uporablja več kompromitiranih naprav ali botnetov za ustvarjanje prevelikih zahtevkov ali prometa. Glavni cilj ni kraja podatkov, temveč povzročitev motenj v delovanju ciljne organizacije.

▷ Sabotaža procesa

Ti napadi se osredotočajo na procese, ki so odvisni od podatkov in so bistveni za nemoteno delovanje. S spreminjanjem ali brisanjem ključnih podatkov napadi onemogočijo učinkovitost operativnih protokolov. Zamislite si npr. vozni park vozil, ki deluje po strogem urniku vzdrževanja. Če bi bili zapisi o vzdrževanju spremenjeni ali izbrisani, bi bila lahko ogrožena pripravljenost vozil, kar bi lahko prekinilo celotno dobavno verigo.



Kibernetske goljufije

Gre za skupen izraz številnih nezakonitih dejavnosti, katerih cilj je finančna korist ali ogrožanje podatkov. Taktike vključujejo uporabo elektronske pošte in tehnik socialnega inženiringa za izkoriščanje ranljivosti v organizaciji, kar pogosto privede do škodljivih posledic. Protiukrepi morajo vključevati zanesljive protokole za preverjanje pristnosti, programe ozaveščanja zaposlenih in nadzorne sisteme za odkrivanje nenavadnih dejavnosti.

▷ Kraja gesel

Gre za eno najosnovnejših oblik kibernetskih goljufij, ki se pogosto kaže v poskusih lažnega pridobivanja podatkov prek e-pošte, telefonskih klicev ali celo besedilnih sporočil. Običajno gre za nujno zahtevo po preverjanju računa. Ozaveščenost je v tem primeru prva obrambna linija - prave finančne institucije ali vladni organi nikoli ne bodo zahtevali osebnih podatkov prek tovrstnih sporočil.

▷ Prevzem računa

Do prevzema računa (angl. Account Takeover ali krajše ATO) pride, ko zlonamerni akter prevzame nadzor nad legitimnim računom (bančnim, e-poštnim, družabnim) brez dovoljenja njegovega lastnika. Pogosto je to mogoče z izkoriščanjem pomanjkljivosti pri preverjanju pristnosti ali varnostnih ukrepih. ATO je lahko še posebej škodljiv za organizacije, v katerih je mogoče profile strank v zunanjih aplikacijah monetizirati, na primer v programih zvestobe.

▷ Goljufije pri plačilih

Plačilne goljufije, ki so pogosto povezane z ogrožanjem poslovne e-pošte, so namenjene nedovoljenim finančnim transakcijam. Nepridipravi se običajno izdajajo za zaupanja vredno osebo in zahtevajo od zaposlenih, ki izvajajo plačila, da spremenijo bančne podatke za plačilo, ki je v teku. Čas je pogosto skrbno načrtovan tako, da sovpada z obdobji, ko je pozornost lahko zmanjšana.

Napačne informacije

Gre za obliko napada, ki vključuje namerno razširjanje lažnih ali zavajajočih informacij z namenom zavajanja, manipuliranja ali povzročanja zmede – gre za orodje za manipuliranje z javnim mnenjem. Te kampanje pogosto uporabljajo spletne kanale, kot so družbeni mediji, elektronsko pošto in spletna mesta.

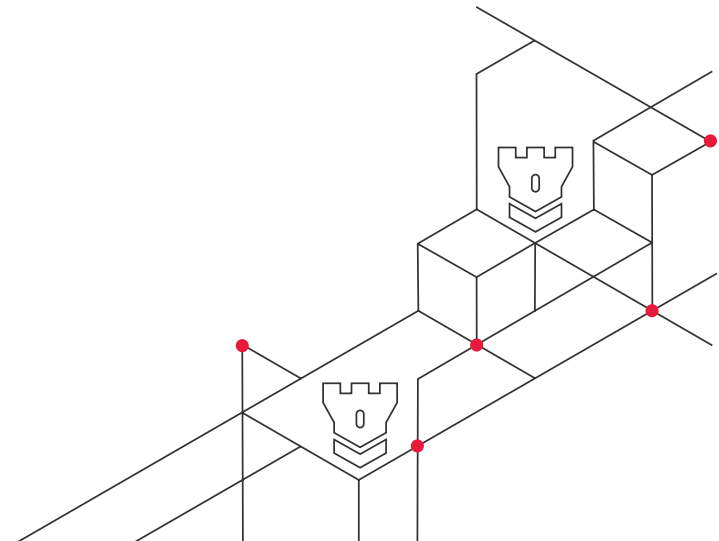
Učinki napačnih informacij so običajno obsežni, od izgube javnega zaupanja in verodostojnosti do dejanske finančne ali družbene škode. Boj proti njim zahteva večplasten pristop, ki vključuje pozornost vseh vpletenih posameznikov in kolektivno ukrepanje. Z uporabo zmogljivosti vaše organizacije za zaščito pred digitalnimi tveganji, kot je obveščanje o kibernetskih grožnjah, lahko zgodaj odkrijete napačne informacije in jih odpravite ter tako zmanjšate njihov vpliv. Glavne vrste taktik dezinformiranja so:

▷ Zloraba blagovne znamke

Kibernetski kriminalci ali zlonamerni akterji lahko z napačnimi informacijami okrnijo ugled blagovne znamke. To lahko vključuje širjenje lažnih mnenj in informacij, ustvarjanje lažnih računov v družabnih medijih, ki se izdajajo za blagovno znamko, ali vzpostavitev goljufivih spletnih mest, ki so podobna pravim. Takšne taktike lahko zmedejo stranke, škodijo blagovni znamki in imajo običajno tudi finančne posledice.

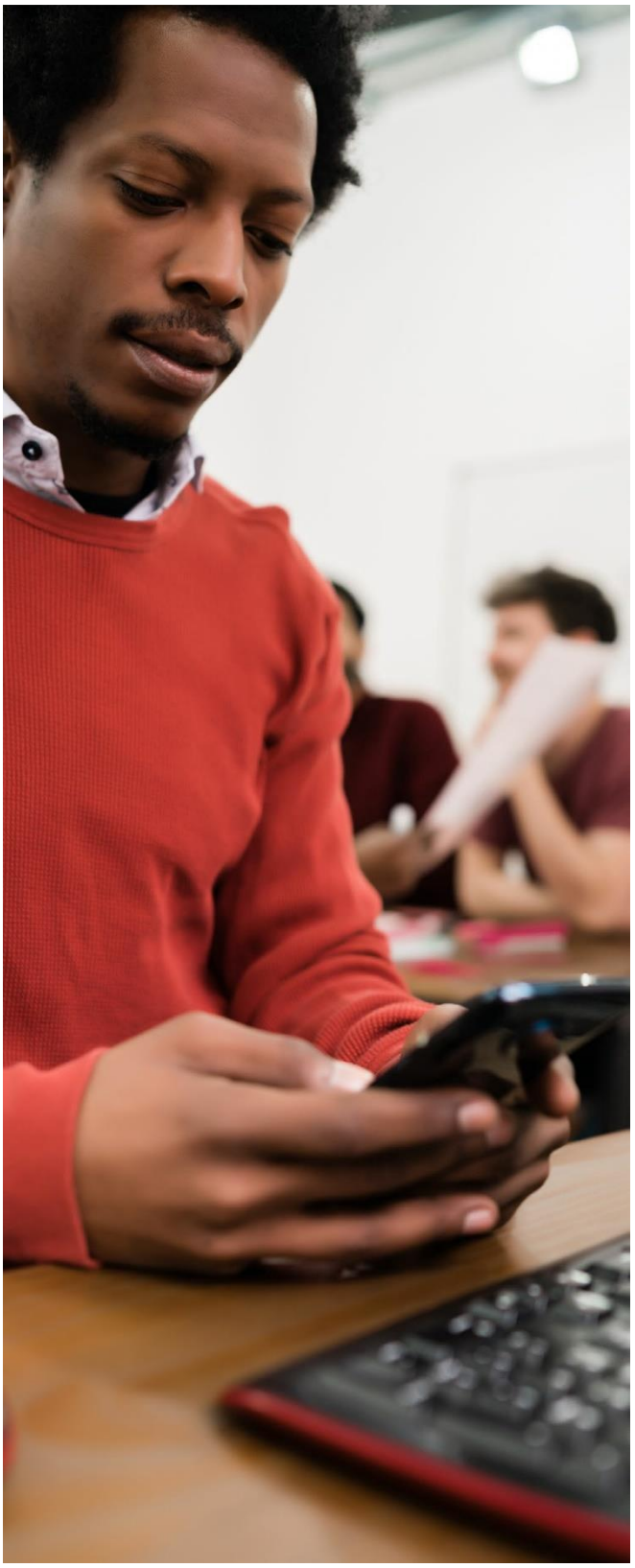
▷ Goljufije na volitvah

Dezinformacije so lahko tudi orožje, ki moti demokratični proces. Za zavajanje volivcev, spodkopavanje kandidatov ali manipuliranje z izidi volitev se lahko širijo lažne zgodbe ali prirejeno gradivo.



Dobre prakse kibernetske varnosti

- Prvi korak k zaščiti je ozaveščanje o tveganjih. Izvedite ciljno usmerjene ukrepe za zaščito informacijskih virov organizacije z ugotavljanjem ranljivosti in morebitnih vrzeli v varnostni infrastrukturi.
- Spremljajte svojo izpostavljenost z uporabo obveščevalnih podatkov za zgodnje odkrivanje groženj, na primer s spremljanjem nezakonitih spletnih tržnic in forumov, kjer kibernetski kriminalci pogosto trgujejo z ukradenimi podatki.
- 24 ur na dan spremljajte in upravljajte vedenje omrežja ter tako preprečite nepooblaščen vstop v svojo sistem ter tako zmanjšajte tveganje kibernetskih groženj in ogroženost podatkov. .
- Ohranite skladnost z razvijajočimi se predpisi o zasebnosti in varnosti ter se izognite pravnim in finančnim posledicam.
- Izvedite oceno neprekinjenega poslovanja in odpornosti. Ocenite zmožnost organizacije in vaših ključnih dobaviteljev, da ohranite delovanje med motnjami in zagotovite neprekinjeno poslovanje ob morebitnih kibernetskih grožnjah.
- Kibernetska tveganja uskladite s splošno poslovno strategijo, kar bo upravam in lastnikom pomagalo pri sprejemanju optimalnih odločitev in učinkovitem razporejanju sredstev. Preberite naš prvi članek v seriji: Kako lahko uprave izboljšajo svoje znanje o kibernetski varnosti: šest strategij za zaščito organizacije pred kibernetskimi grožnjami.
- Zapletenost področja kibernetskih groženj kaže, da reševanje kibernetske varnosti ni izključno v domeni IT-oddelkov. Namesto tega gre za skupno odgovornost, ki zahteva celovito strategijo upravljanja tveganj.



Kako lahko pomaga BDO

BDO-jeva ekipa za kibernetsko varnost se zaveda tveganj, povezanih s tehnologijo, in ponuja celovit nabor storitev za zagotavljanje kibernetske varnosti. Naš pristop vključuje temeljito oceno vaše stopnje zrelosti kibernetske varnosti, testiranje vašega omrežja na ranljivosti in celovito oceno tveganja. Še danes se dogovorite za posvetovanje z našo ekipo.

BDO je Microsoftov globalni varnostni partner leta 2024 in vodilni ponudnik rešitev kibernetske varnosti za podjetja. Zagotavljamo celovite rešitve z uporabo naprednih varnostnih in identitetnih zmogljivosti Microsoft 365 in Microsoft Azure Security.

Manuela Šribar
manuela.sribar@bdo.si