12 opazovanih incidentov kibernetske varnosti v letu 2018

Članek je pripravil BDO Singapur in je preveden v slovenski jezik

December 2018

BDO team za kibernetsko varnost je na podlagi pregledanih več incidentov kibernetske varnosti na lokalni ravni kot tudi regijsko, pripravil naslednjih 12 primerov, ki so rezultat sodelovanja naših strank, partnerjev in združenj. Ob tej priložnosti bi se zahvalili našim strankam in partnerjem za njihovo podporo pri pripravi in predstavitvi tega prispevka.

1. Izključitev interneta ali motnje delovnega procesa?

Ugotovljeno je bilo, da nekatere organizacije trdno stojijo za tem, da so nekateri deli poslovanja brez dostopa do interneta. Ta trdna naravnanost je bila izbrana iz razlogov, da bi zaščitili ključne podatke in sisteme pred zunanjimi ali celo notranjimi kibernetskimi grožnjami.

Vendar pa so te organizacije s tem povzročile motnje pri svojem poslovanju. Tako stališče so zavzele brez skrbne preučitve vpliva na vsakodnevne operacije (kar so prav hekerji hoteli). Nekateri premišljeni zaposleni so tako zaobšli ovire s svojo mobilno napravo za dostop do interneta. Na žalost bi to lahko ustvarilo še eno možnost za napad, saj ni nadzorovana oz. ima omejen nadzor IT varnostne ekipe.

2. Popravki do smrti

V fazi kritičnih poslovnih operacij kjer bi lahko neuspeh IT sistemov bil katastrofalen ali ogrožen s strani hekerjev, nekatere organizacije izberejo »patch-at-cost« pristop.

Tveganje se tako še poveča zaradi številnih različnih aplikacij, sistemov in platform, ki se izvajajo skupaj. To se še poslabša, kadar se ad-hoc krpanje izvede zunaj obdobja načrtovanega vzdrževanja, pri čemer ni dovolj časa, brez ustreznega testiranja predlaganih popravkov ali pa se politike in postopki ne upoštevajo ustrezno. Izpadi sistema se lahko pojavijo, ko so popravki hitri in niso izvedeni v skladu s predpogoji in postopki.

Posledično postane zaznana grožnja informacijskim sistemom bistvena grožnja, ki povzroča neupravičene izpade sistema. Eden glavnih kibernetskih tveganj je, da poskušate obravnavati vsa potencialna tveganja, in to je ponazoritev, kjer lahko takšno ukrepanje postane kontra produktivno.

3. Najnovejša in najboljša tehnologija

Organizacije nenehno pregledujejo svojo varnostno držo in zlasti po resnem incidentu v zvezi s kibernetsko varnostjo lahko organizacija poskuša popraviti "zlomljeno ograjo" in tako postane plen množice prodajalcev. Medtem ko je vodilna rešitev na trgu priporočljiva s strani različnih priznanih ponudnikov, pa ni nujno, da služi namenu predvsem zaradi edinstvenega okolja določene organizacije.

Veliko ICS/SCADA/OT sistemov je licenčnih in delujejo na osnovi ustavljenih in starejših različicah operacijskih sistemov v proizvodnjah, na primer. Verjetno ne bi bila dobra ideja, če bi poskušali uvesti nove tehnologije, ki konstantno zahtevajo povezave z oblakom ter se periodično posodabljajo in s tem prekinjajo delovanje CPE sistemov.

Veliko ICS/SCADA/OT sistemov je licenčnih in delujejo na osnovi ustavljenih in starejših različicah operacijskih sistemov v proizvodnjah, na primer. Verjetno ne bi bila dobra ideja, če bi poskušali uvesti nove tehnologije, ki konstantno zahtevajo povezave z oblakom ter se periodično posodabljajo in s tem prekinjajo delovanje CPE sistemov.

To bi lahko uvedlo nove kibernetske grožnje, ki bi licenčne sisteme izpostavilo novim in neznanim kibernetskim grožnjam v oblačnih sistemih.

4. BIG data prihajajo z večjo odgovornostjo do zasebnosti podatkov

Gospodarstvo 4.0 je nedvomno usmerjeno v podatke in s prevzemom oblakov, orodij za analizo podatkov in platform, so naredili ekipo FANG (Facebook, Amazon, Netflix, Google) za neprimerljive voditelje analitike podatkov. Njihove storitve so zdaj na voljo številnim uporabnikom prek preproste naročnine v oblaku. Od spletnega nakupovanja ali prenosa filmov, priporočil za aplikacije, ki omogočajo skupno rabo, se zdi, da te čarobne platforme vedo, kaj kupec išče še pred začetkom samega iskanja. Vsa to »čarobnost« izhaja iz analize ogromnih količin podatkov, pridobljenih iz socialnih medijev, spletnih iskanj in celo komunikacij med posamezniki.

Vendar pa Splošna uredba EU o varstvu podatkov (GDPR) in številni drugi lokalni predpisi o zasebnosti jasno določajo, da mora biti vsaka organizacija, ki zbira podatke od posameznikov, eksplicitna pri pojasnjevanju namena zbiranja in uporabe podatkov ter, da mora pridobiti ustrezno soglasje ob zbiranju podatkov. Zaradi tega pridobivanje velikih količin podatkov, zbranih od posameznikov, prinaša dodatne obveznosti glede zasebnosti podatkov, ki se jih številne organizacije ne zavedajo ali niso pripravljene prevzeti.

5. Digitalna transformacija v devetih nebesih

V preteklem letu so vlade in ponudniki storitev v oblaku združili prizadevanja za pomoč malim in srednje velikim podjetjem (MSP) pri prehodu v oblak, da bi spodbudila agilnost in inovacije na platformah v oblaku za digitalno preoblikovanje. Medtem ko so ponudniki storitev v oblaku na splošno naredili oblačne platforme bolje zavarovane in bolj odporne, kot to počnejo podjetja na svojem dvorišču, je pomembno razumeti eno od ključnih načel v poslovnem / IT outsourcingu – delitev nalog. Podjetje je na splošno odgovorno za podatke/aplikacije, ki so v oblaku.

S tem, ko podjetje podatke in aplikacije prestavi v oblak se glede varnosti postavi v boljši položaj zaradi dodatnih varnostnih zaščit, ki jih izvaja ponudnik storitve v oblaku – popravki, končne točke, varnostne kopije, spremljanje in opozorila. Vendar pa mora podjetje prevzeti lastništvo varstva podatkov, varnostno držo in higieno v oblaku pa je potrebno pregledati in revidirati s tako natančnostjo, kot jo imajo v podatkovnih centrih.

6. Varnost z negotovostjo

V nasprotju pa še vedno obstajajo lastniki podjetij, ki menijo, da so njihova podjetja mala in ne dovolj poznana, da bi lahko postali tarča kibernetskih hekerjev. Tako mnenje so si ustvarili zato, ker so njihovi sistemi in procesi zastareli ter bolj analogni kot digitalni, hkrati pa so dobro zavarovani s svojim težko razumljivim načinom razmišljanja.

Zlasti stari Microsoft Windows operacijski sistemi, ki delujejo nezaželeno in nezavarovano, so kot časovna bomba. Microsoft ne vzdržuje in ne izdaja več popravkov za operacijske sisteme na koncu svoje življenjske dobe (in zatorej tudi na koncu podpore).

Kibernetskim hekerjem še vedno uspe priti tudi do sistemov, ki delujejo v okolju z zračno režo in jih izkoristiti, kot smo videli v kršitvah podatkov, ki se pojavljajo v zdravstveni industriji.

Poleg tega se današnji kibernetski hekerji zavedajo, da mala in srednja podjetja (MSP) v dobaviteljski verigi zagotavljajo storitve in so povezana z velikimi podjetji, zato jim predstavljajo lažji prodor in vstop do njih.
Zato je za velika podjetja zelo smiselno, da vzpostavijo nadzor nad zunanjo politiko in uveljavijo neko obliko preverjanja in usklajevanja z zunanjimi partnerji, s tem pa sebi zagotovijo večjo skrbnost in varnost poslovanja.

7. Ničelno zaupanje, razumevanje in stik

V nedavnem pregledu politike varstva podatkov v podjetju, ki izvaja storitve za pomoč uporabnikom in storitve za popravila mobilnih telefonov, so vzpostavili sistem za izbris vseh podatkov o strankah na mobilnem telefonu, takoj ko jim je bil ta predložen v popravilo.
S to politiko varstva podatkov z ničelnim zaupanjem in ničelnim stikom, podjetje svojim strankam zagotovi, da organizacija in njeni zaposleni niso odgovorni za kakršno koli zbiranje podatkov in kakršno koli upravljanje z njihovimi napravami.
Od njihovih strank se pričakuje, da bodo podatki na mobilnem telefonu redno podprti, da se le ti ob ponovnem stiku s podjetjem lahko obnovijo na popravljenem telefonu.

Tak pristop je bil uporabljen za določitev osnove, za zaščito podjetja in zadev pomembnih za poslovanje ter za vzpostavitev pripravljenosti za odkrivanje in odzivanje na dogodke, ki bi jih lahko ogrozili. Organizacija je pri varstvu podatkov strank odlično ravnala v skladu s svojo politiko, pri izvajanju poslovnih storitev in pri analizi izkušenj strank, pa rezultati niso bili tako spodbudni.

To je verjetno povzročilo nezadovoljstvo strank, ki morda nimajo opravljenih varnostnih kopij in bodo po opravljeni storitvi oziroma po popravilu izgubili vse podatke.
Ničelno razumevanje in presoja položaja kupca pa ne sovpada s končnimi porabniki, uporaba takega pristopa pa kot posledico nosi izgubo določenega deleža strank.

8. Veriga je močna kot njen najšibkejši člen

Pri pregledu kakršnih koli incidentov v povezavi s kibernetsko varnostjo in s kršitvijo podatkov, sta ključna dva pogosta dejavnika:

- Napačna konfiguracija sistemov in tehnične napake
- Pomanjkanje ozaveščenosti končnih uporabnikov

Za informacijske sisteme podjetja lažje vzpostavijo nadzor in varnostne politike, procese ter ljudi, za zaščito teh sistemov, končne uporabnike pa je po drugi strani težje nadzorovati in so lažje tarče za kibernetske hekerje. S prevlado BYOD sistema v podjetjih (prinesi svojo napravo .. nekateri pravijo tudi prinesi lasten propad) velik delež naprav ni upravljan in lahko dostopajo do poslovnih podatkov, kot so e-poštna sporočila in baza datotek, kar predstavlja vse več potencialnih ciljev za kibernetske hekerje.

Če želi podjetje okrepiti varnostno držo in zgraditi kulturo kibernetske odgovornosti, se mora izogibati ukrepov, ki zahtevajo velik napor osebja za spoštovanje kompleksnih varnostnih nalog. Predlagan pristop omogoča učenje pozornosti in vzpostavitev odprtega kanala za povratne informacije, ki opozarjajo na morebitne nepravilnosti.

9. Hranite le kar je potrebno in zahtevano; manj je več

V današnjem gospodarstvu, ki temelji na podatkih, podjetja prek omni-channel točk dostopajo do zbirke podatkov o svojih strankah in opravljajo številne eksperimente digitalne marketinške kampanje, ki vplivajo nanje. V skladu s politiko varstva zasebnih podatkov, uredbo EU o varstvu podatkov in z različnimi lokalnimi in regionalnim zakoni na tem področju morajo podjetja zbrati dovolj podatkov le za predvideno uporabo in namen; velja načelo manj je več.

Z ukinitvijo platforme za socialna omrežja Google+, po nepravilni objavi uhajanja podatkov o uporabnikih, je Google imel srečo, da je zbral le podatke, ki so bili ključni za njegovo delovanje, brez dodatnih osebno določljivih podatkov uporabnikov.

V Združenih državah Amerike ne obstaja zakon, ki bi Google zavezoval k objavi razkritja podatkov uporabnikov, ampak ti zakoni v Ameriki obstajajo le na lokalni ravni. V Kaliforniji, kjer ima Google sedež, morajo podjetja razkriti podatke le, če vključujejo ime posameznika in številko socialnega zavarovanja, številko osebne izkaznice ali vozniško dovoljenje, registrsko tablico, zdravstvene podatke ali podatke o zdravstvenem zavarovanju.

V primeru da incident, ki je razkril osebne podatke uporabnikov, ni bil razkrit organom, lahko nastopijo resnejše posledice in ukrepi oblasti.

10. Kar ne veš, te ne bo bolelo… ali te bo?

Ukrepi za kibernetsko varnost so namenjeni zaščiti pred sedanjimi in potencialnimi kibernetskimi grožnjami. Obramba pred temi grožnjami je težka, predvsem če se teh groženj ne zavedamo, še huje pa je, če ne vemo ali smo njihova tarča ali ne.

V preteklem letu, smo opazili porast zagonskih podjetij, ki ponujajo storitev spletne varnosti in obveščanja na podlagi podatkov, ki so zbrani iz Surface, Deep in iz Dark Web-a. Njihov namen je pomagati podjetjem, pri pregledu krajinskih pregledov z ustreznimi podatki, na podlagi katerih kasneje ugotovijo, ali se nahajajo na križišču katere koli skupine kibernetskih hekerjev. Nekatera zagonska podjetja pa danes ponujajo tudi storitev za odpravo oziroma ublažitev kibernetskih groženj.

Pregledovanje in spremljanje prejetih groženj s tega področja je zelo preudarno, a morajo podjetja paziti, da jih to prekomerno ne omejuje. Podjetje mora imeti vzpostavljen model groženj, ki pregleduje vse nevarnosti in ranljive točke podjetja, hkrati pa pomaga pri določitvi primernega odziva na zadevano grožnjo.

11. Internet stvari ALI internet groženj

IS (internet stvari) naprave so vtkane v današnji tesno povezan svet, ki se je razvil v ogromno tehnologijo, vendar pa razvoj informacijske tehnologije, ki prihaja na mainstream, prinaša tudi ranljivosti, ki jih je potrebno dobro razumeti, če želimo dano tehnologijo učinkovito izkoristiti. Velika podjetja, proizvajalci in trgovci na drobno iščejo načine za izkoriščanje platforme interneta stvari, ki združuje zbrane analitične podatke z naprednimi sistemi poročanja. Inovacije, medsebojna povezanost in oblikovanje kibernetske varnosti so ključni dejavniki za spodbujanje vrednosti ekosistema interneta stvari.

“Koliko IS naprav obstaja v današnjem povezanem svetu, s koliko napravami si izmenjujemo podatke? Koliko ljudi ima dostop do teh podatkov in kakšne odločitve se sprejemajo s temi podatki?”

To je nekaj vprašanj, na katere ne bomo imeli odgovora, a bodo za naš povezan svet predstavljali resno grožnjo.
12. oktobra 2016 je prišlo do masovne porazdeljene zavrnitve storitev (DDoS), ki je imela vpliv na nedostopnost interneta za velik del vzhodne obale ZDA.
Napad, katerega so se oblasti sprva bale, naj bi bilo delo sovražne države, v resnici pa je bilo delo Mirai botnet-a. To je zgodba o nenamernih posledicah in nepričakovanih varnostnih grožnjah, ki veliko pove o naši moderni družbi.

Glede na to da so IS naprave namenske (pomeni da imajo ozek izbor funkcij), je potrebno nadzorovati komunikacije zunaj standardnega nabora, strokovnjaki za IT pa morajo hitro preiskovati komunikacije, ki jih običajno v svojem omrežju ne vidijo. Analiza omrežnega prometa je primerna za obravnavo teh vrst napadov a zahteva tesno sodelovanje strokovnjakov za varnost in za omrežje, za ublažitev že ugotovljenih groženj. Nenazadnje bi morala podjetja revidirati IS naprave v svojem omrežju, in zagotoviti, da so bila neveljavna gesla spremenjena in uporabljena po potrebi s čim manj privilegiji.

12. Ali podjetje potrebuje kibernetsko zavarovanje?

Popolno preprečevanje kibernetskih napadov je napačno.

Skupina za kibernetsko varnost organizacije ne more popolnoma in celovito zavarovati pred napačno konfiguracijo, zasledovalci IT,

tretjimi osebami, človeškimi napakami in goljufivimi zaposlenimi. Poleg notranjih groženj, pa veliko večjo nevarnost predstavljajo zunanje grožnje, ki se nenehno spreminjajo, podjetje pa jih ne more nadzorovati.

"Ne gre za vprašanje, če, ampak kdaj?", Strokovnjaki in analitiki v industriji so to izjavo pogosto navajali v razpravi o kibernetskih napadih.

Velika in mala podjetja so bila in bodo še naprej napadena. Kibernetski napadi za podjetje predstavljajo velik strošek. Izguba podatkov in zaupnih informacij, ki vodijo v motnje poslovanja in kršitve predpisov, ne bodo stale podjetja le ogromne globe. Pomembnejša je izguba zaupanja in zvestobe strank zaradi okrnjenega ugleda podjetja.

Podjetje lahko na kibernetsko zavarovanje gleda kot na dodatno zaščito. Kibernetski paketi zavarovanja, ki so na voljo danes, pomagajo podjetju

minimalizirati izgubo v primeru kibernetskega napada. Ti paketi zagotavljajo tudi zaščito pred stroški povezanimi s:

- Krajo podatkov
- Izsiljevanjem in odkupninami
- Hekingom
- Napadi z ohromitvijo storitev
- Kriznim managementom
- Pravnimi zahtevki in storitvenimi sanacijami

Kibernetsko zavarovanje pa ne more nadomestiti najboljših praks podjetja za kibernetsko varnost, lahko pa pripomore k zagotavljanju večjega miru, nekaterim podjetjem pa tudi pri obnovi storitev pomembnih za poslovanje. Čeprav se podjetje morda ne more popolnoma pripraviti na razne kršitve, lahko sprejmejo ukrepe za ublažitev tveganj, povezanimi z nakupi kibernetskega zavarovanja kot dodatne zaščite.

Kot opomnik našim strankam in partnerjem moramo vsi pregledovati našo higieničnost kibernetske varnosti in drže, pomembno pa je, da izboljšamo morebitne vrzeli med politikami, procesi in celo med ljudmi.

Vedno smo pripravljeni in sposobni ponuditi svoje strokovno znanje in podati nasvete, ki vam bodo pomagali pri zagotavljanju svoje zavarovanosti in zanesljivosti.

www.bdo.com.sg