KIBERNETSKA VARNOST

10 KLJUČNIH TRENDOV IN PRIPOROČIL ZA LETO 2019

Prispevek je pripravil BDO Belgija in je preveden v slovenski jezik.

10 KLJUČNIH TRENDOV ZA LETO 2019

1. Zamegljenost glavnih akterjev kibernetskih groženj

Organi kazenskega pregona in obveščevalne agencija poročajo o povečanem sodelovanju med skupinami nacionalnih hekerskih napadov in organiziranimi kriminalnimi združbami po vsem svetu, zlasti na Kitajskem, v Rusiji, Iranu in Severni Koreji.

2. Povečanje poslovnih napadov na elektronsko pošto (BEC)

Hitra rast napadov na podjetja na področju socialnega inženiringa, predvsem v obliki plačil računov neustreznim dobaviteljem.

3. Rast Spear-Phishing (usmerejnih) e- poštnih napadov

Povečano število napadov s spear-phising-om, ki so usmerjeni predvsem v vodstvene delavce, zlasti direktorje in kontrolorje nepooblaščenega elektronskega prenosa sredstev.

4. Rast napadov z izsiljevalskimi virusi

V preteklem letu so se napadi z izsiljevalskimi virusi povečali za 350%, predvsem v zdravstveni industriji.

5. Izkoriščanje hekerskih napadov, ki temeljijo na dobavni verigi

Znatno povečanje števila kršitev kibernetskih podatkov zaradi začetnega nepooblaščenega dostopa prek omrežnih povezav tretjih dobaviteljev do glavnih izvajalcev.

6. Priznanje, da regulativna usklajenost s standardi kibernetske varnosti ne zagotavlja resnične varnosti

Mnoga podjetja so vlagala v zagotavljanje skladnosti z različnimi standardi kibernetske varnosti (npr. PCI-DSS, HIPAA, ISO27001 itd.). Kljub temu pa se je potrebno zavedati, da skladnost predpisov s splošnimi zahtevami glede varnosti informacij ne zagotavlja, da podjetje ne bo utrpelo velike kršitve glede kibernetskih podatkov.

7. Višji stroški kršitev kibernetskih podatkov = višje zavarovalne premije za zavarovanje kibernetske odgovornosti

Ker se povprečni stroški kršitev kibernetskih podatkov zadnjih pet let povečujejo, se tudi stroški zavarovalnih premih za zavarovanje kibernetske odgovornosti.

8. Vedno bolj kompleksna ureditev kibernetske varnosti

Regulativno področje pogostokrat zaostaja in to še posebej velja za področje kibernetske varnosti, ki ga po naravi zaznamujejo nestanovitnost in hitrost tehnoloških inovacij. Zakonodaja kibernetske varnosti je zelo zapletena in poteka na različnih ravneh: nacionalni in mednarodni brez ustrezne harmonizacije na svetovni ravni. Zato je ključnega pomena, da podjetja danes predvidevajo zakonodajno okolje za jutri.

9. Pomanjkanje izkušenih strokovnjakov na področju kibernetske varnosti

V svetu primanjkuje izkušenih, usposobljenih in certificiranih strokovnjakov za kibernetsko varnost, da bi zadovoljili vedno večje povpraševanje po svetovalnih storitvah za kibernetsko varnost in upravljali varnostne storitve po vsem svetu.

10. Izgorelost zaradi hekerskih napadov vpliva na naložbe v kibernetsko varnost

Zaradi stalnih poročil o množičnih hekerskih napadih na mednarodni ravni, vedno več podjetij postaja apatičnih do potencialnega vpliva na njihovo podjetje, pri čemer pogosto domnevajo, da je samo nakup povečanega zavarovanja kibernetske odgovornosti zadosten, namesto da vlagajo v poskus preprečevanja napada.

KLJUČNA PRIPOROČILA ZA LETO 2019

1. Izvedite oceno nevarnosti e-pošte

Glede na naraščajoče število hekerskih napadov prek sistemov elektronske pošte, podjetja vedno pogosteje želijo izvajati ocene nevarnosti e-pošte, zlasti za zaznavanje zlonamerne programske opreme, ki jih protivirusni programi in požarni zidovi niso odkrili.

2. Opravite oceno ogroženosti omrežja in končnih točk

Z razširitvijo informacijskih sistemov, aplikacij programske opreme, lastnih naprav in internet stvari (IoT), organizacije vedno bolj preizkušajo svoje omrežje in končne točke z ocenami groženj z uporabo naprednih sistemov za odkrivanje vdorov (IDS), da bi zmanjšali potencialne ranljivosti za kibernetske naprave.

3. Izvedite Spear-Phishing (usmerjevalne) kampanje

Zaradi znatnega povečanja napadov s spear-phising-om bi morale organizacije občasno preizkusiti kibernetsko ozaveščenost in dovzetnost svojih zaposlenih za kibernetske napade prek vključenih certificiranih etičnih hekerjev, ki lahko izvajajo vaje za spear-phising na osnovi socialnega inženiringa.

4. Opravite oceno ranljivosti in testiranje prodora

Večina organizacij, bodisi interno ali najema zunanje neodvisno podjetje, da opravi oceno ranljivosti s pomočjo programske opreme za skeniranje zlonamerne programske opreme in izvede testiranje prodora za odkrivanje potencialnih zunanjih ranljivosti za kibernetske napade. Pomembno je, da se te teste izvaja enkrat letno, še bolje pa je dvakrat ali četrtletno glede na nenehen razvoj kibernetskih napadov.

5. Izvajati učinkovit in pravočasen program upravljanja s popravki programske opreme

Najpomembnejše kršitve kibernetskih podatkov v zadnjih dveh letih so bile posledica dejstva, da organizacije niso izvajale učinkovitega in pravočasnega programa upravljanja s popravki programske opreme Microsoftovih in Cisco programskih paketov.

6. Vzpostaviti program ozaveščanja o kibernetski varnosti/izobraževalni program

Stroškovno učinkovit način za izboljšanje kibernetske varnosti je ustvarjanje človeškega požarnega zidu z zagotavljanjem kakovostnih izobraževalnih programov za kibernetsko varnost za vse zaposlene, od vrha podjetja do dna.

7. Izvedite oceno kibernetske varnosti

Pomembno je, da se neodvisno preveri, ali so politike, načrti in postopki za kibernetsko varnost organizacije zadostni za ustrezno zaščito digitalnih sredstev organizacije in za zagotovitev skladnosti z ustreznimi standardi kibernetske varnosti.

8. Izvajajte program za odzivanje na nesreče (IR)

Bistvenega pomena je, da ima vsaka organizacija dobro premišljen in periodično preizkušen program odzivanja na incidente (IR), vključno: s politikami, načrti, postopki, standardnimi obrazci in periodične vaje/simulacije.

9. Zagotovite stalno spremljanje, odkrivanje in odziv (MDR)

Vsaka organizacija mora vlagati v ustrezno raven MDR storitev na podlagi kibernetskih groženj s katerimi se srečuje. Ključno je, da se hitro odkrijejo vdori in se zajamejo ter odpravijo škodljive programske opreme, da se zmanjšajo negativni vplivi na informacijski sistem in podatkovna sredstva.

10. Investirajte v načrtovanje neprekinjenega poslovanja/obnovo po nesreči, da zagotovite odpornost

Glede na veliko verjetnost kršitve kibernetskih podatkov je bistveno imeti zanesljiv in varen sistem za varnostno kopiranje podatkov, da se zagotovi minimalen vpliv na operativno učinkovitost organizacije in zaščito najbolj dragocenih podatkovnih sredstev pred izgubo ali poškodbo.

POVZETEK

Kako lahko BDO pomaga

Kot neodvisni svetovalci ocenjujemo vaše obstoječe okolje ob upoštevanju specifik vašega podjetja.

Pripravimo pregled vaših prednosti in slabosti na strukturiran način in z uporabo razumljivega jezika, tako da imate dobro predstavo o obstoječih tveganjih.

Naš pristop je postopen, najprej poskrbimo, da bodo obravnavane največje ranljivosti obstoječe varnosti. Šele, ko postavimo trdne temelje, naredimo korak naprej z opredelitvijo dodatnih pregledov.

Za ljudi, ki niso tehnični, ni lahko pridobiti vpogled v dejanska kibernetska tveganja. V vlogi samostojnih strokovnjakov smo upravljavski odbor in poskrbimo, da boste še naprej videli gozd skozi drevesa.

Medtem, ko je bi razvoj počasen, je hitrost v današnjem svetu nenadna. Vendar pa izhodišče ostaja nespremenjeno: samo tisti, ki se prilagodijo, bodo preživeli. Z veseljem vas bomo vodili pri oblikovanje pravih izbir v vašem kibernetskem razvoju.

KONTAKT

STEVEN CAUWENBERGHS
partner
Risk Advisory Services

E-mail : steven.cauwenberghs@bdo.be
Tel : +32 497 05 12 23

FRANCIS OOSTVOGELS
manager
Risk Advisory Services

E-mail : francis.oostvogels@bdo.be
Tel : +32 474 92 08 00

NICK HUYSMANS
supervisor
Risk Advisory Services

E-mail : nick.huysmans@bdo.be
Tel : +32 486 31 90 45