IIA Bulletin

Vidik notranjih revizorjev glede današnjih najbolj perečih vprašanj *Februar 2020*

PONOVNO RAZMISLIMO O PRIPRAVLJENOSTI: PANDEMIJA IN KIBERNETSKA VARNOST

Epidemija koronavirusa prinaša osredotočenost na problematiko, ki je pogosto prezrta od organizacij - neprekinjeno poslovanje in pripravljenost na katastrofe.

Negotovost glede obsega in trajanja trenutne epidemije že vpliva na organizacije, da ponovno ocenjujejo načrte potovanj zaposlenih ter do živčnih vlagateljev, ki prodajajo zaloge. Tveganje za širitev izbruha pandemije bi moralo biti v mislih pri vodjih podjetij in vodjih notranje revizije, saj ima to tveganje vpliv na dobavne verige, produktivnost zaposlenih in odnose s tretjimi osebami. Vsaj vodje notranje revizije bi morali biti pripravljeni pregledati in priporočiti potrebne posodobitve glede pandemije, pripravljenosti na nesreče in načrtov neprekinjenega poslovanja.

Čeprav so organizacije v prvih fazah ugotavljanja potencialnih vplivov koronavirusa na njihovo delovanje, se pojavlja dodatno tveganje - socialni inženiring sredi krize. Kibernetski kriminalci izkoriščajo vse večjo zaskrbljenost nad smrtonosnim virusom. Po poročanju TechRadar Pro, britansko spletno mesto za novice in preglede o potrošniški tehnologiji, so se v treh japonskih prefekturah pojavile elektronske pošte o navodilih glede koronavirusa, ki so skrivale zlonamerno programsko opremo. Hekerji so prikrili zlonamerno programsko opremo v e-poštnih prilogah, ki naj bi vsebovale informacije za zaščito pred širjenjem virusa. Namesto tega je v prilogi bil naložen virus druge vrste, poroča TechRadar Pro.

Kibernetski kriminalci, ki izkoristijo krizo, so nekaj, kar bo verjetno postalo bolj razširjeno. Organizacije morajo opredeliti svoje protokole in prakse za obrambo pred socialnim inženiringom, kot so lažno predstavljanje, pretvarjanje in privabljanje.

Splošna vprašanja za oceno pripravljenosti organizacije na nesreče

V nadaljevanju je nekaj splošnih vprašanj, ki si jih mora vaš oddelek notranje revizije zastaviti, ali se vaša organizacija pravilno ukvarja s pripravljenostjo na nesreče in načrtovanjem neprekinjenega poslovanja:

- Kdaj so vaši ključni deležniki na zadnje pregledali načrte neprekinjenega poslovanja vaše organizacije? Kdaj ste na zadnje preizkusili načrte vaše organizacije in kdo je to izvedel?
- Kakšne postopke vsebujejo vaši trenutni načrti v primeru nastopa naravnih katastrof, pandemij ali drugih morebitnih motenj, ki bi lahko vplivali na vaše objekte, zaposlene, ponudnike oblakov, dobavitelje, kupce?
- Kdaj je vaša organizacija na zadnje pregledala pogodbe s poslovnimi partnerji za neprekinjeno poslovanje?
- Kako so prodajalci, regulatorji, zavarovalne agencije in drugi ključni deležniki obveščeni o spremembah reševanja naravnih katastrof, pandemij ali drugih morebitnih motenj?
- Kako sposobna je vaša organizacija izvajati poslovno kritične avtomatizirane aktivnosti ročno? Ali so na voljo potrebni obrazci in priročniki s postopki? Ste za to ustrezno usposobljeni?
- Kako pogosto vaša organizacija preverja kritičnost različnih poslovnih procesov in se tako prepriča, da je vrstni red obnovitve primeren? Kako oddelek za IT zagotavlja, da so kritične komponente infrastrukture na razpolago, da se upoštevajo zahteve za oživitev poslovanja?
- Kateri poslovni cilji bi bili moteni, če ne bi bilo dostopa do interneta ali mobilne telefonije?
- Kakšno usposabljanje so vaši zaposleni in poslovni sodelavci izvedli o tem, kaj storiti v primeru naravne nesreče ali pandemije?
- Ali je vaš podatkovni center in/ali vaš ponudnik oblakov zmožen "izklopiti luči", kar pomeni, da dalj časa ni prisotnih nobenih delavcev?
- Katerih poslovno kritičnih procesov ali dejavnosti ne bi bilo mogoče prenesti na nadomestno lokacijo? Kateri imajo regulativne posledice glede na čas ali trajanje dogodka?

Splošna vprašanja za oceno vaše ranljivosti na področju socialnega inženiringa

V nadaljevanju je nekaj splošnih vprašanj, ki si jih mora vaš oddelek notranje revizije zastaviti, da bi ugotovil, kako je vaša organizacija ranljiva na področju socialnega inženiringa:

- Katere so prakse, politike in usposabljanja vaše organizacije glede nevarnosti socialnega inženiringa? Kako te sporočate zaposlenim in kako jih uveljavljate?
- Ali je grožnja socialnega inženiringa popolnoma razumljena in sporočena vsem ravnem zaposlenih v vaši organizaciji?
- Kateri sistemi in procesi so še posebej izpostavljeni socialnemu inženiringu? Na katere ključne poslovne procese lahko vpliva?
- Kakšno testiranje izvaja vaš oddelek za IT v zvezi s področji posebne ranljivosti socialnega inženiringa?
- Ali načrtujete notranjo revizijo področij, ki jih ima vaša organizacija na področju socialnega inženiringa?

IIA VIRI (V ANGLEŠČINI)

Knowledge Brief

- Strategic Public Asset Protection

Practice Guides

- Assessing the Risk Management Process
- Auditing Third-Party Risk Management
- Coordination and Reliance: Developing an Assurance Map
- Business Continuity Management
- GTAG: Business Continuity Management
- GTAG Assessing Cybersecurity Risks

Internal Auditor magazine

- In the Face of Nature