KAJ BI MORALI DIREKTORJI VEDETI IN NAREDITI GLEDE KIBERNETSKE VARNOSTI

Znano je, da lahko kršitve kibernetske varnosti vplivajo na zaposlene, kupce,procese in tehnologijo podjetja, pri čemer IT strokovnjaki in direktorji pogosto delajo skupaj, da bi sisteme po napadu vzpostavili v prvotno stanje. Medtem, ko se številni vidiki kibernetske varnosti ukvarjajo s tehnologijo, je vedno večja potreba, da direktorji v organizacijah, zlasti v srednje velikih podjetij, prevzamejo odgovornost za svoj program kibernetske varnosti. Poglobljena vključenost direktorjev lahko pozitivno vpliva na metodologijo kibernetskega tveganja. Direktorji lahko prispevajo k dodani vrednosti strategije kibernetske varnosti, z osredotočanjem na kritična področja, kot so tveganje, skladnost, poročanje, vrednotenje poslovanja in ERP.

Bi se radi o tem pogovorili z nami?

01 53 00 920, info@bdo.si

10 KLJUČNIH VPRAŠANJ, KI BI JIH MORALI DIREKTORJI ZASTAVITI INFORMATIKOM IN ODGOVORNIM ZA KIBERNETSKO VARNOST

1. Kakšne je splošna nevarnost organizacije glede kršitve podatkov v smislu verjetnosti nastanka in finančnega vpliva?

2. Kakšno naj bo kibernetsko zavarovanje za optimalno zaščito podjetja?

3. Kakšni so povprečni stroški kršitve podatkov v naši panogi?

4. Kakšne so denarne kazni za neupoštevanje specifičnih regulativnih zahtev kibernetske varnosti?

5. Kakšni so stroški skladnosti, ki se nanašajo na zahteve za kibernetsko varnost in/ali posebne zahteve iz pogodb?

6. Ali je iz finančnega vidika bolje imeti urejeno kibernetsko varnost strojne opreme, programske opreme in ostalih storitev znotraj podjetja, ali je bolje to prepustiti zunanjemu izvajalcu?

7. Komu lahko zaupamo, da nam svetuje, ko pride do pomembnih napadov ali kršitev podatkov?

8. Katere informacije v povezavi s kibernetskim tveganjem in preventivnimi ukrepi naj bi bile poročane poslovodstvu?

9. Ali ima podjetje ustrezne ljudi za sprejem poslovnih odločitev glede kibernetske varnosti?

10. Ali mora podjetja vključiti tudi zunanje strokovnjake za področje kibernetske varnosti in/ali svetovalce z izkušnjami na področju odzivanja na kibernetske incidente in pripravo in obdelavo kibernetskih zahtevkov.

10 KLJUČNIH UKREPOV, KI BI JIIH INFORMATIKI MORALI SPREJETI

1. Sodelovati tesno z direktorji in upravnim odborom, da se zaposli izobražen, izkušen, certificiran kader na področju informacijske tehnologije in kibernetske varnosti, ki bo deloval kot odgovoren za področje informacijske varnosti.

2. Najem neodvisnih podjetij, da redno izvajajo naslednje: ocene e-poštne kibernetske nevarnosti, ocene spletnih grožnje, ocene ranljivosti, preizkušanje penetracije in ciljno usmerjene kampanje, ki so namenjene zbiranju podatkov o dejanskem stanju trenutne ravni kibernetske varnosti organizacije.

3. Sodelovanje z ostalimi oddelki, da se oceni kibernetska tveganja vseh funkcionalnih področij organizacije.

4. Ustvariti ustrezno stroškovno ravnotežje med informacijsko tehnologijo, upravljanjem informacij, tveganjem, varnostjo in skladnostjo.

5. Zagotoviti ustrezen program za varovanje podatkov in program za zaščito notranjih informacij.

6. Preveriti pravočasen in učinkovit program za upravljanje popravkov programske opreme.

7. Zagotoviti ustrezen dostop do informacij, njihovo shranjevanje, posredovanje in neprekinjeno poslovanje.

8. Prizadevati si ustvariti kibernetsko varnost v celotni organizaciji.

9. Predajte izvajanje storitev spremljanja, zaznavanja in odzivanja (24x7x365) izkušenemu zunanjemu ponudniku varnostnih storitev.

10. Zagotoviti pravočasno poročanje o vseh kršitvah podatkov.

ZAKLJUČEK

Popolnoma jasno je, da nekateri direktorji nimajo dovolj znanja s področja kibernetske varnosti. Prav tako jim ostali odgovorni ne posredujejo ustreznih informacij o kibernetskem tveganju kateremu je njihova organizacija vsakodnevno podvržena. Veliko direktorjev se zaveda kibernetske nevarnosti, vendar se zaradi različnih razlogov, ne odločajo pravilno kaj je potrebno storiti za zmanjšanje verjetnosti kibernetskih napadov v njihovi organizaciji.

KAJ BI MORALI DIREKTORJI VEDETI IN NAREDITI V ZVEZI S KIBERNETSKO VARNOSTJO

Na podlagi vrste razprav z direktorji iz različnih gospodarskih panog, vključno iz finančnega sektorja, zdravstvenega varstva, vladnih ustanov, avtomobilske industrije, proizvodnje, zasebnega kapitala in odvetniških pisarn je postal jasno, da obstaja vrzel me tako v znanju, kot v aktivnostih za kibernetsko varnost. Iz the razprav so bila tri najpogostejša vprašanja s strain direktorjev:

1. Kaj naj bi direktorji sploh morali vedeti o kibernetski varnosti?
2. Kaj naj direktorji vprašajo svoje informatike in odgovorne za kibernetsko varnost o kibernetski varnosti?
3. Kaj naj bi informatiki morali narediti glede kibernetske varnosti?

Ključno je, da direktorji postavijo kibernetsko varnost kot prioriteto v njihovi organizaciji in predstavijo, da je odgovornost na tem področju vsakega posameznika. Vzpostavitev kulturo kibernetske varnosti se je izkazala kot najboljša obramba proti kibernetskim napadom. Ljudje in ne tehnologija so najmočnejši ali najšibkejši člen proti kibernetskim napadom. Na direktorjih je trenutno, da si pridobijo dovolj znanja s tega področja, da bodo znali sprejeti ustrezne ukrepe za zaščito njihovih najdragocenejših informacij.

Seveda direktorji ne morejo postati certificirani strokovnjaki za varnost informacijskega sistema. Direktorji morajo povečati svoje znanje o ključnih konceptih kibernetske varnosti in izkoristiti lastne vodstvene sposobnosti za strateško zasnovo in upravljanje tveganj ter kako najbolje vlagati svoj čas in sredstva za izboljšanje kibernetske obrambe.

10 KLJUČNIH ZADEV, KI NAJ BI JIH DIREKTORJI VEDELI O KIBERNETSKI VARNOSTI

1. Katere so tiste informacije, ki so za podjetje najbolj pomembne? Kibernetski napadi in varnostne kršitve se bodo še naprej pojavljale in bodo negativno vplivale na poslovanje. Trenutno znaša povprečna cena učinka kibernetske kršitve 7,5 milijona ameriških dolarjev po podatkih Ameriške komisije za varnostno izmenjavo (SEC).

2. Kakšno zavarovanje kibernetske odgovornosti je potrebno za finančno zaščito premoženja podjetja.

3. Kakšno je tveganje za kibernetsko kršitev: po večini raziskav kibernetske varnosti, več kot 60% vseh kršitev podatkov izhaja iz nepooblaščenega dostopa enega od trenutnih zaposlenih v organizaciji, nekdanjih zaposlenih ali dobaviteljev tretjih oseb.

4. Ali je vaša organizacija ustvarila program notranjih varnostnih groženj, ki ublaži tveganje za kibernetsko kršitev znotraj organizacije?

5. Doseganje skladnosti informacijske varnosti z enim ali več standardi za varnost informacij (npr. ISO 27001, NIST 800-171, HIPAA, NYDFS, AICPA-SOC itd.) je dobro, vendar ne zadostuje za zagotavljanje resnične kibernetske varnosti. Kakšne ukrepe bi morala sprejeti vaša organizacija za zagotovitev resnične kibernetske varnosti?

6. Ali je organizacija izvedla neodvisno oceno ogroženosti elektronske pošte in omrežja. Če je bila nedavno izvedena, kakšni so bili rezultati?

7. Ali je organizacija pridobila neodvisno oceno ustreznosti kritja zavarovanja za kibernetsko odgovornost. Premije za zavarovanje kibernetske odgovornosti znatno povečujejo stroške in pogosto ne pokrivajo vseh škod, ki jih povzroča kibernetska kršitev.

8. Upravljanje varnostnih storitev za nadzorovanje, zaznavanje in odzivanje mora biti združeno, da bi zagotovili resnično varnost informacij in odpornost podatkov. Ugotovite, ali notranji viri za izvajanje nadzora, zaznavanja in odzivanja delujejo, ali jih je treba oddati zunanjim izvajalcem. Če je tako, koliko bo to stalo?

9. Ugotovite, ali ima organizacija celovit sistem odzivanja na incidente, obnove po nesreči in načrte neprekinjenega poslovanja.

10. Razmišljajte o različnih scenarijih: če nas napadejo izsiljevalci, ali bi plačali odkupnino? Če je odgovor pritrdilen, koliko bi bilo potrebno predvideti? Ali bo pokrita z zavarovanjem kibernetske odgovornosti?