ENDURSKOÐUN
Þórarinn Ólason
Sérfræðingur hjá Ernst & Young

Stjórnun netöryggis – Ábyrgð stjórnar og stjórnenda

Félag löggiltra endurskoðenda

Eru stjórnarmenn, auk hins almenna stjórnanda, nógu meðvitaðir um ábyrgð sína í að mynda og samræma heildstæða nálgun félagsins að netöryggismálum?

Í nútíma markaðsumhverfi reiða félög sig sífellt meira á tækni og er svo komið að upplýsingatækni er nú undirstöðuþáttur í rekstri hvers félags. Um leið og upplýsingatækni gerir félögum kleift að bæta rekstur og þjónustu, t.d. með því að safna upplýsingum og greina þær, ber tæknin þó einnig með sér þá áhættu að geta orðið félögum að falli.

Segja má að öryggisrof (e. breach) og gagnalekar séu eitthvað sem flestir þekkja til og samkvæmt könnunum hefur árleg aukning í tilkynningum verið um 50% á alþjóðavísu undanfarin ár. Þetta eru svo sem ekki fréttir fyrir stærri félög sem fylgjast virkt með slíkum árásum en þó sýna kannanir að félög eiga sífellt erfiðara með að fylgja hraðri þróun í upplýsingatækni og mæta þeirri áhættu sem henni fylgir. En hverjar eru afleiðingarnar?

Árlega birtir EY skýrslur um niðurstöður kannana á sviði netöryggismála og ná þær m.a. til stórra og heimsþekktra fyrirtækja. Eftirfarandi er útdráttur úr einni slíkri sem náði til yfir 1.800 alþjóðlegra fyrirtækja frá 60 löndum og úr flestum atvinnugreinum.Helstu efnistök skýrslunnar voru:

- Sífelld þróun og ör aukning í flækjustigi og hraða í netöryggismálum og hvaða þýðingu netöryggi hefur fyrir félagið.
- Nauðsyn aukinnar ábyrgðar og þátttöku stjórnar og stjórnenda, umfram tæknisvið, í netöryggismálum og samþættingu áhættustjórnunar inn í stefnumótun.
- Mikilvægi þess að innleiða heildstæða nálgun við stjórnun netöryggis inn í upplýsingatækniöryggi, byggt á viðeigandi greiningu.

Sameiginleg ábyrgð, skýr skjölun verðmætra upplýsingaeigna og samþætting öryggismála við aðra þætti reksturs eru þannig grundvallaratriði í árangursríkri stjórnun netöryggis. Spurningin er þá: Eru stjórnarmenn, auk hins almenna stjórnanda, nógu meðvitaðir um ábyrgð sína í að mynda og samræma heildstæða nálgun félagsins að netöryggismálum? Samkvæmt könnun EY eru best undirbúnu félögin þau sem hafa nú þegar áttað sig á því að ábyrgðin sem fylgir því að verjast árásum liggur ekki lengur eingöngu hjá yfirmönnum tæknimála, heldur hjá stjórn og stjórnendum og nær til félagsins í heild sinni. Þau félög hafa einnig sagt skilið við nálgun sem byggist á lágmarks viðbúnaði og fylgni við regluverk, „Er þetta nauðsynlegt fyrir okkur?“ eða „Erum við ekki örugg?“, en spyrja sig frekar frumvirkra (e. proactive) spurninga eins og „hvernig getum við tryggt það að okkar verðmætustu upplýsingaeignir séu nógu öruggar?“

Því eins og sagt er þá er þetta ekki spurning um hvort öryggisrof mun koma upp hjá félaginu, heldur hvenær. Það má jafnvel gera ráð fyrir því að í mörgum tilfellum hafi félög ekki áttað sig á því að öryggisrof hefur þegar átt sér stað. Í skýrslu EY kemur meðal annars fram að:

- 56% svarenda töldu ólíklegt eða mjög ólíklegt að félagið hefði burði til þess að uppgötva eða greina háþróaða árás.
- 87% svarenda töldu virkni netöryggis félagsins (e. Cybersecurity function) ekki mæta þörfum þess.
- 61% svarenda taldi félagið ekki hafa samræmt netöryggisstefnu sína og áhættusækni eða þol (e. risk appetite or tolerance).

Í umræðunni um öryggisrof í tengslum við áhættusækni og þol er gott að hafa í huga að þau má í besta falli flokka sem kostnaðarsamt frávik frá megin-starfsemi félagsins en geta í versta falli haft í för með sér alvarlegar afleiðingar eins og rekstrarstöðvun og jafnvel dómsmál.

Ein helsta niðurstaða skýrslunnar er því sú að jafnvel þótt sérfræðiþekking sé enn undirstaða viðbúnaðar þá er það ekki fyrr en að innan félagsins er þróuð almenn meðvitund og samábyrgð á upplýsinga- og netöryggi að stjórnendur geta lagt traust sitt á að mikilvægustu eignir félagsins – upplýsingar – séu verndaðar með viðeigandi hætti.
Mikilvægt er því fyrir félög að vera meðvituð um sífellt aukna netáhættu sem og það að ábyrgð á því að meta og mæta áhættunni með viðeigandi lausnum liggur hjá félaginu öllu, ekki síst stjórn og stjórnendum.

Birt í Viðskipta Mogganum fimmtudaginn 21. apríl 2016 bls. 12.