Kibernetski napadi so draga šola

Čeprav je informacijska varnost osnovna kompetenca digitalne transformacije, je podjetja še ne obravnavajo kot enega največjih tveganj pri sodobnem poslovanju. Koristi vlaganj v informacijsko varnost je resda težko ovrednotiti z vidika prihodka, jih je pa toliko lažje predstaviti z vidika izgube denarja, časa in ugleda. Stroški, ki jih podjetja utrpijo zaradi kibernetskih groženj so pogosto tako veliki, da ogrozijo dobiček in zamajejo plačilno sposobnost, saj lahko dosežejo tudi milijonske zneske. E-izobraževanje o informacijski varnosti na delovnem mestu se v danih razmerah kaže kot ključna informacijsko-varnostna naložba.

V času, ko delovanje organizacij opredeljuje enačba poslovanje=informacijski sistem in se pravzaprav vse ključne poslovne dejavnosti izvaja samo še digitalno, se je obvladovanje poslovnih tveganj razširilo še na polje informacijske varnosti. Slednja ni več problem službe za informatiko ali odgovornih za izvajanje varnostnih politik, temveč se je prenesla na C-raven.

Informacijska varnost danes je oziroma bi morala biti v domeni odločevalcev na najvišji ravni, od generalnega menedžmenta do vodstva financ, kadrov, proizvodnje, prodaje, nabave … Vsi, ki so v upravljanje informacijske varnosti kakorkoli vključeni priznavajo, da so najšibkejši člen ljudje. In zato je informacijska varnost ena prvih kompetenc, ki jo mora podjetje nenehno razvijati in vzdrževati, ko stopa po poti digitalnega poslovanja. Ne verjamete?

Kaj se lahko zgodi, če ne...

Poglejmo si samo nekaj pravzaprav vsakodnevnih groženj, ki izkoriščajo človeški faktor in kaj se zgodi, ko jih zaposleni ne prepoznajo:

- direktorska prevara: gre za enega najbolj preprostih vendar najdražjih primerov socialnega inženiringa. Vodja računovodstva od direktorja dobi elektronsko pošto za nujno nakazilo predujma poslovnemu partnerju v tujini. Običajno gre za nekaj 100.000 evrov. Računovodja nič hudega sluteč nakaže vsoto na TRR tako imenovane mule, ki denar takoj po prejemu pošlje naprej po drugi poti in zakrije sled, ki se zato zelo hitro izgubi. Na tak način je bilo v zadnjih nekaj letih oškodovanih že več podjetij v Sloveniji.

- izsiljevalski virus: o tej vrsti kibernetskih napadov je bilo že veliko zapisanega celo v sredstvih javnega obveščanja, saj so bila napadena tudi že znana podjetja. Uporabnik lahko na službenem ali domačem računalniku odpre okuženo priponko, na primer prejeti račun od poslovnega partnerja ali potrdilo o dostavi spletnega naročila s strani ponudnika hitre pošte. Izsiljevalski virus ne zaklene samo uporabnikovega računalnika ampak se hitro razširi po celotnem poslovnem omrežju ter lahko doseže tudi strežnike s poslovno programsko opremo in računalnike sodelavcev. Podjetja velikokrat plačajo visoke odškodnine, saj v nasprotnem ne morejo več poslovati. Podjetje lahko celo propade, če podatkov ne more obnoviti. Tudi v primeru dobro urejenih procesov varnostnega kopiranja podatkov podjetja običajno utrpijo več dnevni izpad poslovanja, s tem pa prihodek in ugled pri poslovnih partnerjih.

- spletna prevara: uporabnik prejme elektronsko pošto s strani banke, ki ga prosi, za preverjanja podatkov zaradi zakonodaje. V sporočilu se nahaja povezava do ponarejene spletne strani, kjer uporabnik pusti svoje prijavne ter druge plačilne, poslovne in osebne podatke, ki jih nato napadalci uporabijo ali za neposredno oškodovanje uporabnika ali za zaslužek z njihovo preprodajo.

Seveda je tveganj, s katerimi se srečujejo zaposleni, ki sodelujejo v informacijsko podprtih poslovnih procesih in digitalnih postopkih precej več. Izpostavili smo jih le nekaj, kjer je grožnjo težko preprečiti četudi podjetje uporablja najboljšo varnostno programsko in strojno opremo, če ima lastno ekipo za informacijsko varnost ali če najema zunanje storitve varnostno-operativnih centrov.

Najbolj se splača vlagati v e-izobraževanje zaposlenih

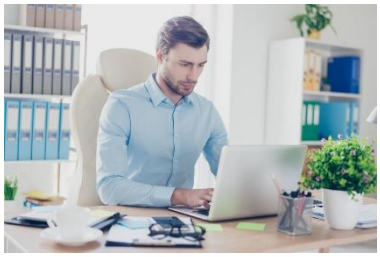
Kot ugotavljajo v organizacijah pa tudi pri ponudnikih varnostnih informacijskih rešitev in storitev, je najbolj učinkovita varnostna naložba usposabljanje zaposlenih. Pri razvoju in vzdrževanju kompetenc na polju informacijske varnosti pa se kot najboljša praksa potrjuje uporaba pristopov e-izobraževanja. Slednje je v tem trenutku zaradi vse večjega obsega oddaljenega dela od doma pravzaprav tudi edina rešitev.

"V celotni ebm-papst grupaciji si že dalj časa prizadevamo za čim višjo stopnjo informacijske varnosti, in pomemben del tega so tudi dobro izobraženi ter osveščeni uporabniki. Zato smo v sodelovanju s podjetjem B2 IT izvedli e-izobraževanje Informacijska varnost na delovnem mestu, ki je na enostaven in poljuden način našim zaposlenim predstavilo najbolj razširjene spletne napade in prevare, ter kako se jim čimbolj učinkovito zoperstaviti," je povedal Robert Manfreda, vodja IT v podjetju ebm-papst Slovenija.

ebmpapst

Uporaba e-izobraževanja omogoča zelo hitro usposabljanje zaposlenih ne glede na kompleksnost, velikost in lokacijsko razpršenost organizacije.

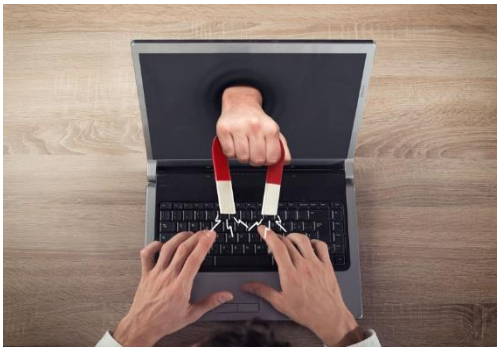
Kot je razložila Mojca Potecin, vodja kadrovske službe v Elektro Celje, je bil cilj e-izobraževanja s področja informacijske varnosti preprečiti varnostna tveganja zaradi neznanja, prevelike ustrežljivosti ali naivnosti posameznikov ter pridobiti izkušnje z izvedbo e-izobraževanj. "Izkazalo se je, da je e-izobraževanje za nas zelo primerno, zaradi lokacijske razpršenosti naših sodelavcev. Pomembno vlogo igra tudi čas, ki so si ga udeleženci razporedili sami, glede na njihove zadolžitve, pri čemer smo vsebinska vprašanja in vprašanja uporabnikov smo reševali strokovno in ažurno".



Poleg tega je tak način zanje še poseben privlačen, saj se ga izvaja digitalno, pravzaprav na enakih medijih, kot jih zaposleni uporabljajo v praksi, ko se morajo varovati pred kibernetskimi grožnjami. Prav zato nekatera podjetja utečene sisteme e-izobraževanja pospešeno razširjajo z usposabljanji za informacijsko varnost.

"Seveda nekatere vsebine kar kličejo po e-izobraževanju, na primer informacijska varnost, ki je menda ne bomo predavali s tablo in kredo," je izpostavil Jani Braune, direktor za pravne, kadrovske in splošne zadeve v podjetju ETI Elektroelement.

Oddaljeno delo tveganja le še povečuje



Zaposleni pri delu od doma velikokrat službene naloge izvajajo na domačih računalnikih, ki so slabše ali sploh niso zaščiteni z varnostno programsko opremo, strojnim požarnim zidom in različnimi drugimi tehničnimi in organizacijskimi ukrepi. Nekatere organizacije so zaposlenim dovolile prenos službenih računalnikov – prenosnikov in namiznih naprav na dom, s čimer so svoja poslovna informacijska sredstva in vire postavila pred branike, s katerimi sicer ščitijo računalniško opremo, sisteme in podatke na lokaciji podjetja. Po drugi strani se je v času pandemije po vsem svetu povečalo število kibernetskih napadov, še posebej takšnih, ki ciljajo na končne uporabnike.

Slednje izpostavljajo praktično vsi ponudniki varnostnih izdelkov ter organizacije, ki se ukvarjajo z informacijsko varnostjo. Po podatkih FBI se je število prijav kibernetskih napadov v času korona krize povečalo za 400% pri čemer na alarmantno stanje opozarjajo v Interpolu. Po njihovih informacijah je bilo februarja in marca letos za 569 odstotka več prijav incidentov, kjer so napadalci uporabili zlonamerne programske kode in spletne prevare, pri čemer je bilo za kar 788 odstotkov več prijav z visokim tveganjem.

Online trening Informacijska varnost za zaposlene

Recept, da se izognete tveganjem in da poskrbite za visok nivo osveščanja zaposlenih iz zadnjih aktualnih kibernetskih napadov je B2 ONLINE usposabljanje iz informacijske varnosti, ki je narejen po najnovejši metodi »learning by doing«.
Metoda namreč zagotavlja maksimalno pomnjenje vsebine, saj so uporabniki vpleteni v učne igre.
V Sloveniji je to edinstven izobraževani program. Z njo se bodo vaši zaposleni naučili:

- pravilno odzvati v realni situaciji morebitnega hekerskega napada,
- kreirati varna gesla,
- ubraniti napadov prek e-pošte ali socialnega inženiringa.

Vas zanima podroben program?

»Cilj e-izobraževanja s področja informacijske varnosti je bil preprečiti varnostna tveganja zaradi neznanja, prevelike ustrežljivosti ali naivnosti posameznikov ter pridobiti izkušnje z izvedbo e-izobraževanj. *Izkazalo se je, da je e-izobraževanje za nas zelo primerno, zaradi lokacijske razpršenosti naših sodelavcev. Pomembno vlogo igra tudi čas, ki so si ga udeleženci razporedili sami, glede na njihove zadolžitve. Sodelovanje z B2 IT je bilo, kot pričakovano, profesionalno in učinkovito. Vsebinska vprašanja in vprašanja uporabnikov smo reševali strokovno in ažurno."*

Mojca Potecin, Vodja kadrovske službe, Elektro Celje d.d.

Želite **demo dostop** do online treninga iz informacijske varnosti za zaposlene?
KLIKNITE!