

Proškolení zaměstnanci jsou nejlepší ochranou firmy

Počet útoků metodami sociálního inženýrství dramaticky roste. Nejefektivnější způsob, jak ochránit firmu, je co nejlépe proškolení její pracovníky. V České republice je nyní dostupná nejmodernější platforma pro komplexní školení zaměstnanců v oblasti security awareness.

Máloco je tak vzdálené skutečnosti jako laické představy o hackerských útocích. A to je problém. Za většinou kybernetických bezpečnostních incidentů dnes nestojí nenechaví mladíci v kapucích, ale dobře organizované skupiny profesionálů. Kybernetické útoky jsou byznys, který funguje jako každý jiný. S řetězcem dodavatelů, outsourcingem a technickou podporou. Prodejním artiklem jsou v tomto případě informace a data.

Stejně tak by byla chyba domnívat se, že primárním terčem dnešních hackerů musejí být vždy jen velké finanční instituce nebo bohaté společnosti. Jakkoli jde o cíle nejlákavější a nejziskovější, útoky často míří i na běžné střední a malé české firmy, úřady či organizace.

Hackerům se daří oklamat firmy podvrženými fakturami

Útoky metodami sociálního inženýrství se staly každodenní realitou. Nejčastější formou je plošný útok – hackeři rozesílají hromadný malware a zkoušejí, kdo se nachytá. Druhou variantou je tzv. spear phishing. V tomto případě se vede útok na firmu prostřednictvím předem vytipovaných zaměstnanců s využitím detailních informací o jejich pracovních aktivitách, zvycích, kontaktech apod.

Metody útočníků jsou čím dál sofistikovanější a ten, kdo si myslí, že jim podlehně jen nepřilíh bystrá či rutinou unavená mysl, se velice plete. Kromě klasického phishingu, činěného nejčastěji formou podvodných e-mailů, jde i o vishing, tedy falešné, věrohodně působící telefonáty, a v současnosti také o útoky s využitím umělé inteligence.

Za pomoci nejmodernějších technologií dokážou útočníci zfalšovat nejenom hlas, ale dokonce i obličej, což je v době, kdy řada firem komunikuje kvůli koronaviru prostřednictvím videokonferencí, alarmující fakt. Cílem všech těchto aktivit je dostat dotyčného pod tlak, zmást ho, prezentovat se jako důvěryhodná či povoláná osoba, získat



Společnosti spadající do výše uvedených odvětví snížily počet selhání zaměstnanců o 88 % během 12 a více měsíců díky kombinaci security awareness školení a simulovaných phishingových útoků. (Založené na vážených průměrech ve společnostech bez ohledu na jejich velikost.)

jeho hesla, přihlašovací údaje, donutit ho udělat krok, který je v rozporu s jeho zájmy či se zájmy jeho zaměstnavatele.

V současné době se lze také čím dál častěji setkat s případy, kdy se kyberzločincům daří české společnosti zmást podvrženou fakturou, kterou zasílají pod hlavičkou některé z dodavatelských firem, samozřejmě s falešnými platebními údaji.

Systém ochrání proškolení zaměstnanci

Obranný val každé firmy je tak silný, jak silný je jeho nejslabší článek. A tím vždy byl, je a bude člověk. Nabízejí se dvě řešení. Prvním je zakázat zaměstnancům telefonovat a používat e-mail. Tím druhým je své lidi proškolení. Udělat ze slabiny přednost. Praxe ukazuje, že poučení zaměstnanci, kteří dokážou správně reagovat, můžou být velice efektivní ochranou firemního prostředí.

Služby security awareness poskytované společnostmi AEC kombinují použití nejnovějších technologií se znalostmi z pedagogiky a psychologie. Obsahují nejen komplexní učení zahrnující zpracovaná videa, e-learning, podrobná on-line školení, ale i řadu dalších unikátních metod. S jejich po-

mocí se daří účastníky zaujmout natolik, že se téma kybernetické bezpečnosti stává přirozenou součástí kultury dané firmy.

Důležitou složkou vzdělávacích služeb AEC je zkušenost vlastním prožitkem. V řadách specialistů společnosti jsou odborníci na argumentaci a vyjednávání, kteří umějí vést falešné telefonáty jak v českém, tak v anglickém jazyce. Experti AEC dovedou simulovat nejrůznější typy kontrolovaných útoků, díky nimž si ověří, jak jsou zaměstnanci schopni čelit kybernetickým hrozbám.

Na základě získaných informací pak lze pracovat s každým zaměstnancem individuálně, hodnotit jeho reakce, monitorovat nesnáze a odpovídajícím způsobem ho doučovat potřebným znalostem. Jednou z věcí, které takový přístup umožňují, jsou pokročilé technologické nástroje, jimiž AEC disponuje. Například díky partnerství se společností KnowBe4, která je lídrem v oboru vzdělávání v oblasti kybernetické bezpečnosti. Právě její platforma dokáže jedinečným způsobem propojit testování s učením, a docílit tak požadovaných a trvalých změn v přístupu zaměstnanců.

Více informací na www.socialing.cz