Výzkum a nové technologie v kybernetické a informační bezpečnosti

Účinnost vzdělávacích phishingových kampaní v čase

(21. 09. 2020, zdnet.com) Akademici z několika německých univerzit testovali účinnost vzdělávacích phishingových kampaní v čase. Zaměstnanci státní správy byli proškoleni na problematiku a nebezpečí a rozeznávání phishingu a poté rozdělení do několika skupin. V rámci těchto skupin byli poté zaměstnanci po určité době přezkoušeni, zda rozpoznají phishingový email. Nejlepších výsledků dosáhla skupina, která byla otestována po nejkratší době od proškolení, a to po 4 měsících. Skupiny otestované po 6 a více měsících od školení již dosahovaly výrazně horších výsledků. Výzkumníci také sledovali jaká forma školení je nejúčinnější. Došli k závěru, že nejlepšími formami jsou interaktivní nebo video školení. Školení ve formě textu (byť i krátkého) má poté efektivitu výrazně menší.

Komentář: Phishing představuje jednu z výrazných kybernetických hrozeb a lze očekávat, že tomu tak bude i v následujících letech. Podvodné emaily přitom útočí primárně na uživatele z řad zaměstnanců a kvalitní vzdělávání tak může výrazně snížit možnost úspěchů útočníků. Pokud tedy účinnost těchto školení takto výrazně klesá v čase tak je třeba, aby školení kybernetické bezpečnosti uživatelů probíhala opakovaně. Na základě předloženého výzkumu je poté zřejmé, že ideální frekvencí pro opakování školení by mělo být 6 měsíců.

Průzkum komunity hackerů a jejich motivace k hackování

(29. 09. 2020, finbold.com) Průzkum organizace Finbold se zaměřil na průzkum toho, jaká je motivace hackerů k jejich činnosti. Průzkum byl plně anonymní a zúčastnilo se jej více než 3 000 respondentů z více než 120 zemí. Překvapivým zjištěním je především to, že až 74% hackerů se dopouští kybernetických útoků, protože to považují za výzvu a 51% ze všech dotazovaných navíc uvedlo, že páchají kybernetické útoky, aby otestovali své schopnosti a znalosti. Podobný počet (49%) navíc hackuje „pro zábavu“. Vedle motivace hackerů se průzkum zaměřil i na to jak dlouho se již této činnosti věnují. 30% z respondentů se hackování věnuje pouze krátkou dobu (1 – 2 roky). Těch, kteří se tomuto oboru věnují více, než 15 let bylo již pouze 5%. Dalšími zjištěními průzkumu je především to, že některé skupiny hackerů již využívají umělou inteligence (AI) jako jeden z nástrojů pro své útoky.

Komentář: Tento průzkum potvrdil to, že komunita hackerů se stále vyvíjí a je dobře schopna adaptovat se na nové technologie (v současné době především umělou inteligenci a technologie 5G). Tento fakt jen podtrhuje potřebu organizací mít dostatek kvalifikovaných odborníků na kybernetickou bezpečnost. Ti jsou v současné době značně nedostatkoví a například dle ENISA jich v EU v roce 2019 chybělo téměř 300 000.

Rostoucí nebezpečí a schopnosti ransomwarových útoků

(30. 09. 2020; scmagazine.com) Společnost Microsoft se vyjádřila k rostoucímu problému s ransomwarovými útoky. V posledním roce se ransomware stal jedním z hlavních problémů, které řeší kybernetický bezpečnostní tým Microsoftu. Problém vidí především v tom, že většina firem vidí ransomware pouze jako formu malwaru a snaží se jej řešit pouze technicky. Důležitou součástí „úspěšného" ransomwarového útoku je však i role člověka (zaměstnance). V rámci zprávy byla také předložena případová studie úspěšného ransomwarového útoku, kde prvním krokem útočníků bylo získání přístupových údajů jednoho řadového zaměstnance a tím i přístupu do virtuální sítě organizace. Zde se poté útočníci snažili získat přístupové údaje více privilegovaných uživatelů, odinstalovat antivirový program a posléze se jim podařilo i implementovat ransomware do systému.

Komentář: Současné útoky „vyděračského malwaru" jsou stále více cílenější a sofistikovanější. NÚKIB v říjnu vydal i analýzu hrozeb plynoucích z ransomwaru, jenž doplnila dříve vydaná doporučení. Pro úspěšný ransomwarový útok je stále více stěžejní role lidského faktoru. Ta je často v kybernetické bezpečnosti podceňovaná. Je důležité, aby byly zaměstnanci každé organizace kvalitně a periodicky v této oblasti vzděláváni.

Nový kvantový způsob komunikace mezi více uživateli

(07. 09. 2020; helpnetsecurity.com) Výzkumníci z Bristolské univerzity vyvinuly nový kvantový přenos dat mezi více uživateli. Tento nový způsob by měl být „absolutně bezpečný" v nastupující době kvantových technologií. Nová technologie funguje na principu rozdělení světelných částic tak, že ke každému příjemci putuje jedna z částí. Snižuje se tím potřeba mít pro každého příjemce individuální odesílací prvek. Tato technologie navíc dokáže fungovat i v rámci existujících přenosových soustav (především v rámci sítí založených na optických vláknech). Výzkumníkům se podařilo síť založenou na této technologii vytvořit za méně než 300 000 britských liber, což je nesrovnatelně méně, než činily náklady jiných obdobných projektů.

Komentář: Přenos dat využívající kvantové počítače je dnes velmi plodnou oblastí výzkumu. Budoucí masové nasazení kvantových komunikačních technologií a vzniku kvantového internetu s sebou však nese i značná rizika. Podobné výzkumy, které dokáží zvýšit bezpečnost kvantové komunikace, jsou tedy stěžejní pro zabezpečení v dohledné budoucnosti.

PETR MARTINEK; p.martinek@nukib.cz
Oddělení výzkumu a evropské spolupráce, NÚKIB