ALISON

Trojica kybernetických hrozieb 2020 a bonus ku každej z nich

Internetová konektivita rastie a s ňou aj zraniteľnosť sietí, prístrojov, mobilných zariadení a dát. Či už ide o priemyselné odvetvia, autá, dopravu, zdravotníctvo alebo verejnú správu, počet kybernetických útokov v roku 2019 narástol niekoľkonásobne. Čaká nás špecializácia kybernetického zločinu, dekáda zvaná dátová a rozvoj technológií v segmente deep fake.

Kybernetický zločin sa špecializuje

V roku 2019 bolo oficiálne hlásených viac ako sto veľkých ransomware útokov vo verejnom sektore v porovnaní s 51 nahlásenými v predchádzajúcom roku. Priemerná platba za výkupné sa v roku 2019 zvýšila 6-násobne. Ak bude tento trend pokračovať aj v roku 2020 (čo určite bude), predpokladá sa cielenie na konkrétne odvetvia, miestnu samosprávu a verejné služby. Firmy a vlády v súčasnosti radšej a ticho platia výkupné. Je to ešte stále lacnejšie, ako sa pokúšať škodu napraviť.

Zločinecký biznis má aj svoje označenie: kybernetická kriminalita ako služba - Cybercrime-as-a-Service (CaaS). Tento model uľahčuje vznik nových zločineckých organizácií a zrýchľuje činnosť existujúcich. Umožňuje útočníkom rýchly prístup k službám a produktom vrátane škodlivého softvéru, zneužitia, služieb na prenájom DDoS, prístupov RDP a botnetov.

Dátová dekáda

Odborníci nazvali rok 2019 *Rokom dátových prielomov*. V dôsledku porušenia údajov bolo dostupných takmer 6 miliárd záznamov vrátane čísel kreditných kariet, domácich adries, telefónnych čísel a ďalších citlivých informácií. Nehody prevádzkovateľov sociálnych sietí, platobných kariet, doručovacej služby, finančných domov. Ako sa hovorí v brandži, „iný deň, iný dátový únik“. Príčinami boli nezabezpečené servery, chyby u prevádzkovateľov služieb, nepostačujúca autentifikácia alebo *multiple and varied failure*.

Digitalizáciou priemyslu, služieb a verejnej správy vznikajú obrovské dátové štruktúry. Sociálne siete, aplikácie a e-shopy zbierajú a analyzujú miliardy údajov. V uplynulých dekádach vznikli stovky veľkých aj menších spoločností na hrane a za hranou zákona, ktoré dáta zbierajú, analyzujú a triedia. A obchodujú s nimi. Spoločnosť Experian zverejnila štatistiky, že sa tak stalo tretine obetí, ktorých dáta unikli.

Deep fake

Falošné videá, falošné nahrávky, falošné správy, všetko pod označením deep fake technologies, všetko vhodné na manipuláciu, vydieranie a ovplyvňovanie verejnej mienky. Rok volieb 2016 sa navždy zapíše do histórie technológií, komunikácie aj politiky.

Sociálne siete sa snažia upratovať a zhadzujú falošné profily, pričom ťažisko ich úsilia je v rozvoji technológií, ktoré dokážu identifikovať deep fake. Kongres USA začiatkom januára schválil finančné prostriedky vo výške 5 miliónov dolárov v rozpočte ministerstva obrany na podporu boja proti zahraničným dezinformáciám. Suma je prioritne určená na stimuláciu „výskumu, vývoja alebo komercializácie technológií na automatické zisťovanie strojom manipulovaných médií“.

ALISON

A neželaný bonus? Osobná bezpečnosť

Pocit osobného ohrozenia sa zvyšuje. Trh bezpečnostných technológií a ich implementácia rastú v niektorých oblastiach až exponenciálne. Prevádzkovatelia sociálnych sietí a médiá si (až oneskorene) uvedomujú ničivý dosah a starý rok sa končil a nový začínal vyhláseniami o blokovaní deep fake formátov, komentárov a politickej reklamy. Neskoro.

Na svetových úložiskách bezpečnostných agentúr a súkromných prevádzkovateľov sú už uložené nevyčísliteľné objemy dát, ktoré budú vedieť spracovať a zužitkovať až budúce technológie. A je úplne jedno, že v čase záznamu dát boli šifrované. Éra kvantová sa už začala v minulom storočí a to znamená, že aj dnes dokonalé šifrovanie bude v budúcnosti prelomené.

Plnú verziu Bezpečnostného reportu 01/2020 nájdete na partnerskom portáli živé.sk.