HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 28. FEBRUÁRA – 2. MARCA 2025

Pocit ohrozenia a realita. Zhodujú sa?

ANKETA

Respondentov od 15 do 65+ rokov sme sa pýtali na ich individuálny pocit ohrozenia. Kyberbezpečnostní profesionáli odpovedajú na základe znalosti. Ktorú situáciu by ste označili ako najviac ohrozujúcu pre používateľov?

Dominik Procházka,
riaditeľ odboru bezpečnosti,
AGEL

Som vždy v ohrození, keď používam počítač a mobil. Prakticky pri každom použití počítača alebo smartfónu sa vystavujeme rizikám. Takmer každý deň sa objavujú nové zraniteľnosti a sofistikovanejšie možnosti pre útočníka.

Tomáš Zaťko,
etický hacker, CEO,
Citadelo

Najviac rizikové je, keď emócie prevezmú kontrolu – v strese či eufórii a v časovom tlaku. Útočníci to dobre vedia. Preto musíme byť ostražití, overovať informácie a zachovávať si chladnú hlavu.

Michal Srnec,
vedúci oddelenia informačnej bezpečnosti,
Aliter Technologies

Kyberpriestor sám osebe predstavuje určité nebezpečenstvo, takže sa domnievam, že najviac sme ohrození práve pri používaní súkromnej komunikácie, chatov a e-mailov. Práve cez tieto kanály sa najviac šíria techniky sociálneho inžinierstva a takto dlhodobo a najčastejšie dochádza k prienikom do systémov či iným podvodným aktivitám. Áno, môže ísť o zneužitie karty alebo inú „finálne podvodnú aktivitu", no až neuveriteľne veľakrát tomu predchádzajú práve techniky sociálneho inžinierstva.

Tomáš Hettych,
viceprezident,
ISACA

Najväčšou hrozbou pre bežného používateľa je online nakupovanie a platby kartou v neoverených e-shopoch, ktoré lákajú na neuveriteľne výhodné ceny. Následne je tiež problémom aj súkromná a často aj obchodná komunikácia cez sociálne siete, free e-mailové služby, zoznamky, chaty a bežné SMS. Ľudia o sebe zdieľajú príliš mnoho informácií.

Richard Kiškováč,
generálny riaditeľ,
Elkan

Určite je najviac závažná strata finančných prostriedkov. Vzhľadom na využívanie umelej inteligencie útočníkmi a rôzne kombinácie sociálneho inžinierstva sú podľa môjho názoru používatelia v ohrození vždy, keď používajú počítač a mobil.

Tomáš Valenta,
riaditeľ,
Check Point Software Technologies na Slovensku

V ohrození sme v podstate stále. Každá uvedená situácia predstavuje istú úroveň rizika a pri každej z nich existuje riešenie, ako riziko eliminovať. Ak by som mal vybrať, tak najväčšie ohrozenie sú verejné nezabezpečené WiFi siete, ktoré umožňujú odchytávať prihlasovacie údaje alebo platobné informácie.

Andrej Žucha,
generálny riaditeľ,
ALISON Slovakia

Vždy, keď používame mobil, tablet, počítač a nepoužívame zdravý úsudok, sme v ohrození. Súhlasím, že kybernetická bezpečnosť je o technológiách, ale my používatelia konáme pod vplyvom svojich očakávaní, želaní, emócií, skúseností a povinností. Preto pre tému platí, že neexistuje univerzálna rada ani osveta o „pocite bezpečia".

Ivana Lysinová,
konzultantka,
Skupina Cyllium

Väčšina ľudí vníma kybernetické hrozby ako niečo abstraktné, čo sa ich netýka. Odporúčala by som nastaviť si v prvom rade kritické myslenie „som vždy v ohrození", keď používam akékoľvek koncové zariadenie. Či už je to počítač alebo mobil. Opatrnosťou nič nepokazíte. Je dobré zamyslieť sa nad dôveryhodnosťou linku ešte pred tým, ako naň kliknem, naskenujem QR kód alebo poskytnem citlivé platobné údaje.

Katarína Kročková,
právnička,
Kročka & Partners

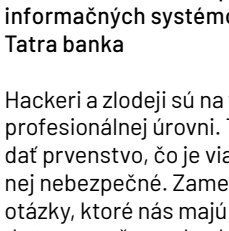
Používatelia sú v kybernetickom priestore ohrození v rôznych situáciách, pričom každá z uvedených možností predstavuje iný typ rizika. Riziko vidím najmä v potenciálnom porušení a zneužití ochrany osobných údajov. Strata kontroly nad týmito údajmi môže viesť k podvodom, ku krádeži identity alebo k finančným stratám.

Marek Zeman,
vedúci oddelenia bezpečnosti informačných systémov,
Tatra banka

Hackeri a zlodeji sú na vysokej profesionálnej úrovni. Ťažko hľadať prvenstvo, čo je viac a čo menej nebezpečné. Zamerajme sa na otázky, ktoré nás majú ochrániť: Je to pre mňa neobvyklá situácia? Musím to urobiť hneď a teraz? Prinesie mi to veľký zisk? Ak si odpoviete pri práci s internetom raz „áno", zvýšte opatrnosť na maximum. Dobrá rada na záver: verejnej WiFi sieti sa vždy vyhýbajte.

Ondrej Kubovič,
špecialista na digitálnu bezpečnosť,
ESET

Bez znalosti kontextu je ťažké povedať, ktorá z hrozieb predstavuje najväčšie riziko – to môže byť iné pre riaditeľa veľkej firmy, influencera, lekára alebo bežného používateľa. Z hľadiska početnosti však naše štatistiky ukazujú, že e-mail patrí k najčastejšie zneužívaným kanálom na šírenie škodlivého kódu, pričom škodlivé a phishingové linky sa môžu posielať aj cez chatové aplikácie či SMS.



Tibor Paulen,
manažér informačnej bezpečnosti,
Stredoslovenská distribučná

Nie je to jednoduché povedať. Vezmime si pre zjednodušenie riziko, že sa dnes zraníte. V princípe sa to môže stať akokoľvek – v kuchyni pri krájaní chleba, lebo nedávam pozor, pri prechádzaní cez cestu, lebo som natrafil na nepozorného šoféra, na schodisku, lebo pozerám do mobilu, a nie pod nohy. To, či sa dnes zraním, závisí od môjho programu, návykov, vonkajších faktorov a aj náhody. Z môjho pohľadu som v ohrození a musím byť v strehu neustále.

Ivan Kopáčik,
bezpečnostný expert,
Gordias

Človek si bežne neuvedomuje, že v kyberpriestore sú ohrozenia oveľa bezprostrednejšie, dômyselnejšie a „neviditeľnejšie" ako vo fyzickom svete. Najväčšie ohrozenie je preto pri aktivitách, ktoré človek celý život robil „fyzicky" – platil v hotovosti, podpisoval sa u notára, nakupoval v kamennom obchode, a bez potrebných znalostí a bezpečnostného povedomia ich teraz začal vykonávať v kybernetickom priestore.

Michal Sekula,
bezpečnostný konzultant,
Eviden Slovakia

Najviac rizík je vo verejnej WiFi sieti. Pri ostatných možnostiach je, alebo by aspoň mala byť nejaká ochrana – šifrovanie, heslá, virtuálna kreditná karta atď. Ale pri verejnej WiFi neviete, ktoré sú legitímne a ktoré sú falošné, akoby „hackerské udičky". A keď je tam ešte možnosť nabíjania mobilu z verejného kábla trčiaceho zo steny, kde je zariadenie na odchytávanie informácií, tak to držím palce.

Timea Tomčová,
manažérka informačnej bezpečnosti,
Poisťovňa Union

Používateľ by mal byť v kybernetickom priestore v primeranej miere obozretný neustále. Napríklad na verejných WiFi sieťach je lepšie vyhnúť sa zadávaniu citlivých údajov, ako sú informácie z kreditnej karty, zatiaľ čo vyhľadávanie verejne dostupných informácií, ako je predpoveď počasia, je menej rizikové. Rôzne situácie vyžadujú rôznu mieru opatrnosti, záleží na kontexte a okolnostiach.

Jaroslav Oster,
predseda správnej rady,
Preventista.sk

Principiálnym problémom je skutočnosť, že práve najohrozenejšia časť používateľov si neuvedomuje nebezpečnosť situácie, v ktorej sa často vo virtuálnom svete ocitnú. Primárne smerujem na seniorné skupiny. Nízka odolnosť voči manipulatívnym technikám predstavuje pre túto skupinu s nízkou úrovňou bezpečnostného povedomia extrémne riziko, čoho dôkazom je neustály nárast počtu obetí a škôd podvodov.

Tomáš Loveček,
prodekan pre vedu a výskum, Fakulta bezpečnostného inžinierstva Žilinská univerzita

Každá operácia vo virtuálnom prostredí nesie určitú mieru rizika. Z možností by som na posledné miesto zaradil elektronickú komunikáciu so štátom a s bankou. Verme autoritám. Aj v súkromí komunikujme, ako by sme komunikovali verejne. Ak zálohujem a využívam autentifikačné prvky, počítam s trhovou cenou počítača. Verejná WiFi je problém. Prvenstvo, ak platím platobnou kartou, a nevyužijem jednorazovú kartu.

Peter Dufek,
manažér kybernetickej bezpečnosti,
Penta Hospitals

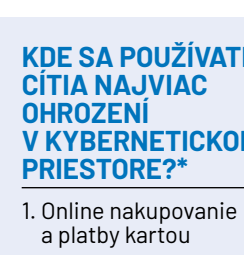
Neexistuje situácia alebo priestor, ktoré by neboli určitým spôsobom ohrozením používateľov. Najviac v ohrození sa môžu ocitnúť pri online nákupoch cez klony známych e-shopov. Sú takmer vernými klonmi a slúžia na krádeže platobných údajov. Rastúcou hrozbou sú phishingové e-maily, ktoré ponúkajú rôzne mechanizmy na sofistikované podvody alebo zavlečenie škodlivého kódu.

Maroš Rajnoch,
architekt kybernetickej bezpečnosti,
Soitron

Hrozby v kyberpriestore nepoznajú hranice ani jazykové bariéry. Podvodníci využívajú SMS, e-maily či sociálne siete a manipulujú obeť pomocou sociálneho inžinierstva. Ochrana spočíva v ostražitosti, zdieľaní informácií v rodine a vo vzdelávaní už od školského veku. Dôležité je naučiť sa rozpoznávať hrozby a v digitálnom svete sa pohybovať bezpečne.

Diana Legdanová,
riaditeľka divízie pre bezpečnosť, Západoslovenská energetika

Za mňa sú dvaja jednoznační favoriti. Používatelia sú ohrození vo verejnej WiFi sieti a hneď za tým je online nakupovanie a platby kartou. Verejnej WiFi sieti neveria už ani deti, keď počujem ich konverzáciu napríklad na letisku. S tým druhým mám osobnú skúsenosť, a to aj napriek dodržaniu všetkých „desatoro" online nakupovania.



Ivan Makatura,
Asociácia kybernetickej bezpečnosti

Namiesto príslovkového určenia miesta „kde" je vhodnejšie pýtať sa „ako". Tiež odpoveď na sugestívnu otázku kde „najviac" je determinovaná tým, „čo" si používatelia najviac cenia. Niekto peniaze, niekto osobné údaje, niekto svoj biznis. Niekto duševné zdravie, o ktoré jeho dieťa príde pri kyberšikane. A niekto život, ak oň nechce prísť vďaka heknutej nemocnici. Škála hrozieb je pestrá. Vyberte si.

Štefan Pilár,
advokát,
Advokátska kancelária Signum

Neexistuje univerzálna a jediná správna odpoveď, lebo tá je závislá od vstupných parametrov. Ak má používateľ na účte desať eur, dosah zneužitia jeho platobných údajov je nižší ako krádež notebooku, ktorý si necháva v kufri auta. Dlhodobo sú však rozšírené zneužitia platobných údajov. Používatelia si pri online platbách často neuvedomujú, že ich kartové údaje sa môžu dostať aj ďalej ako len k príjemcovi platby.

Marián Klačo,
vedúci oddelenia bezpečnosť informácií,
Volkswagen Slovakia

Najriskantnejšie sú verejné WiFi siete, ak si používateľ nechráni svoje údaje napríklad VPN-kou. Hrozby sa tiež šíria v súkromnej komunikácii, takže pozor na podvodné e-maily, esemesky a správy na sociálnych službách.

KDE SA POUŽÍVATELIA CÍTIA NAJVIAC OHROZENÍ V KYBERNETICKOM PRIESTORE?*

1. Online nakupovanie a platby kartou
2. Ukradnutie počítača alebo mobilu
3. Keď som vo verejnej WiFi sieti
4. Pri využívaní služieb elektronického bankovníctva
5. Som vždy v ohrození, keď používam počítač a mobil
6. Súkromná komunikácia mail, chat, SMS
7. Elektronická komunikácia so štátom
8. Nemám nikdy pocit ohrozenia

*úplné údaje na strane 2