**Povoliť firemný počítač alebo mobil na súkromné účely?**

**Odborník radí, za akých podmienok to bude pre firmu bezpečné**

**Bratislava, 20. február 2023 – Takmer 50 % zamestnancov v slovenských firmách je za to, aby využívali firemné zariadenia, ako je mobil a počítač, aj na súkromné účely. Podľa prieskumu spoločnosti Seyfor\* má túto možnosť 37 % opýtaných Slovákov. Odborník odporúča, aby firma pre tieto prípady po bezpečnostnej stránke dobre nastavila nielen firemnú sieť, ale aj každé koncové zariadenie zvlášť.**

Je bežnou praxou, že zamestnávatelia tolerujú alebo povoľujú používanie firemných zariadení, typu mobil a počítač, aj na súkromné účely. *„Zamestnanci prostredníctvom nich najčastejšie riešia súkromnú poštu, spracúvajú osobné dokumenty, nakupujú online alebo vstupujú do súkromných účtov na sociálnych sieťach,“* hovorí Milan Ryšavý odborník na bezpečnosť zo spoločnosti Seyfor.

**Aké sú riziká používania firemných zariadení na súkromné účely**

Odborník upozorňuje, že pre zamestnávateľa predstavuje využívanie firemných zariadení na osobné účely zvýšené riziko, najmä ak sa tieto zariadenia používajú mimo firemnej siete, kde sa rad sieťových bezpečnostných technológií (dostupných vo firemnej sieti) nemôže uplatniť. Je teda potrebné riešiť zabezpečenie priamo na úrovni každého koncového zariadenia, aby bola zaistená adekvátna úroveň ochrany aj mimo firemnej siete (práca z domu a na služobných cestách, na dovolenkách a pod.)

Riziká, ktoré hrozia pri používaní firemných zariadení na súkromné účely, majú štandardné scenáre. Rovnako, ako pri pracovnom režime, najčastejším vektorom útoku býva emailová komunikácia a komunikácia cez sociálne siete. Tzv. phishing cieli na užívateľov, aby získal ich osobné údaje, alebo aby spustil na koncovom zariadení škodlivý softvér. Pokiaľ k nákaze koncového zariadenia dôjde mimo firemnej siete, napríklad doma, je vysoko pravdepodobné, že pri opätovnom pripojení do pracovnej siete bude problém aj tu.

Zamestnanci slovenských firiem v prieskume uviedli spomínaný phishing ako najčastejší bezpečnostný incident (50 %), ktorý sa im stal. Pripojenie zavíreného zariadenia do firemnej siete sa udialo v 38 % prípadov a 22 % zamestnancov zažilo na svojom zariadení útok hackerov.

**Stačia jednoduché pravidlá**

Ryšavý dopĺňa: *„Je zrejmé, že nestačí použiť iba bezpečnostné technológie, ale je nutné zamerať sa aj na vzdelávanie užívateľov, aby vedeli, čo je bezpečné správanie v kyber priestore.“* Konzekvencie voči vzniknutým problémom by mali byť podľa neho prispôsobené konkrétnej spoločnosti a povahe jej práce. Iné pravidlá a interné zvyklosti platia pri technologickom start-upe, iné v silne regulovanom prostredí, akým je vojenské spravodajstvo. Je vhodné interným predpisom jasne definovať, za akých podmienok a akým spôsobom je možné firemné zariadenie použiť na súkromné ​​účely. *„V praxi býva častá situácia že interný predpis toto využitie zakazuje a používanie na súkromné ​​použitie je ale v praxi ticho tolerované. V tomto režime je potom ťažko vymáhateľná zodpovednosť za prípadné škody, ktoré vyplynuli z porušenia pravidiel,“* hovorí Ryšavý.

**Ako správne uchopiť bezpečnosť?**

Zabezpečenie je potrebné riešiť na úrovni každého koncového zariadenia zvlášť, pretože ochrana v rámci firemnej siete už nebýva dostatočná (zamestnanci s koncovými zariadeniami cestujú, pracujú z domu a pod.). Základom je antimalware nástroj s centrálnou správou. Pridať treba správne zabezpečený a priebežne aktualizujúci sa operačný systém, a to vrátane aj pre aplikácie.

Za nadstavbovú, ale dôležitú funkcionalitu, potom môžeme považovať oddelenie firemných dát a dokumentov od tých súkromných, čím vieme zaistiť vyššiu úroveň ochrany pre citlivé firemné dáta. Aj po technickej stránke ponúkajú súčasné digitálne zariadenia vyššiu ochranu pred zneužitím. Odborník odporúča, aby autentifikácia užívateľa pri vstupe do zariadenia bola kombinovaná. *„Základom je silné heslo, ktoré odporúčam kombinovať s identifikáciou užívateľa cez niektorý z biometrických prvkov, ako je otlačok prsta či rozpoznanie tváre,“* uzatvára M. Ryšavý.

\*Zdroj: Prieskum prebiehal v dňoch 8. až 15.11.2022. Autorom prieskumu je agentúra MNFORCE. Reprezentatívna prieskumná vzorka slovenskej populácie podľa pohlavia, veku a kraja: 1 000 respondentov od 18 do 60 rokov, ktorí v práci využívajú informačné a digitálne technológie.

**O spoločnosti SEYFOR**

Seyfor sa radí k veľkým európskym dodávateľom ICT riešení. Spoločnosť má cez 1 600 zamestnancov v ôsmich krajinách a celosvetovo obsluhuje zákazníkov v 38 štátoch. Dlhodobo patrí k najrýchlejšie rastúcim IT spoločnostiam v regióne. Je najväčším výrobcom účtovných, ERP a mzdových a personálnych systémov v Českej republike. V roku 2022 konsolidované výnosy presiahli sumu 125 miliónov eur. Spoločnosť uskutočnila v posledných rokoch desiatky významných akvizícií IT firiem v Českej aj Slovenskej republike a tiež na Balkáne. Ovládajúcimi vlastníkmi spoločnosti sú slovenská private equity spoločnosť Sandberg Capital a Martin Cígler. Firma bola založená v roku 1990 ako Cígler Software, v rokoch 2017 – 2022 pôsobila pod značkou Solitea.

**Kontakt pro média:**

Michaela Raffayová

michaela.raffayova@seyfor.com

+421 948 939 342