č. j. UKRUK/128065/2020
17. 04. 2020

Pokyn č. 5 - Doporučení pro ochranu osobních údajů a minimalizaci hrozeb a rizik při práci s výpočetní technikou, v mobilní komunikaci či na sítích při práci z domova

Doporučení pro zaměstnance

- **Pozor na podvodné e-maily**
- **Neotevírejte podezřelé odkazy v e-mailech**
- **Nezaměňujte pracovní počítač za soukromý**
- **Vyhněte se veřejným Wi-Fi sítím**
- **Přistupujte zodpovědně k volbě hesel**
- **Nepovolujte makra v běžných dokumentech**
- **Nepodceňujte fyzickou bezpečnost počítačů**
- **Kdy kontaktovat Vaši lokální IT podporu?**
- **Kdy hlásit bezpečnostní incident?**

Pozor na podvodné e-maily

V současné době je možné zaznamenat zvýšenou aktivitu hackerů snažících se využít probíhající pandemickou situaci a poptávku jednotlivců po informacích ohledně nového koronaviru. Mezi často využívané prostředky patří rozesílání podvodných e-mailů, které obsahují přílohy či odkazy, které působí jako důležité informace o novém koronaviru.
Podvodný e-mail může vypadat velice důvěryhodně. Cílem těchto útoků je obvykle nekalé získání finančních prostředků či přístupu do informačního systému např. za účelem umístění tzv. ransomware. Následně je vyžadováno výkupné. Účelem takového útoku ale může být i paralyzace celé UK.

Dnes již neplatí, že lze podvodný e-mail poznat podle nedokonalé češtiny. Též se nenechte ukolébat zdáním, že e-mail zasílá osoba, kterou znáte. Pokud se Vám zdá být v jakémkoli případě příloha nedůvěryhodná či žádný e-mail s takovou přílohou neočekáváte, neotevírejte ji. Škodlivý kód se navíc nemusí projevit ihned po spuštění. V případě pochybností se vždy obraťte na Vaši lokální IT podporu.

Neotevírejte podezřelé odkazy v e-mailech

Tzv. phishingový e-mail zpravidla skrývá, kam odkazy vedou. Skrytá cílová cesta odkazu je první znak podvodného e-mailu. Jak zjistit, kam odkaz z e-mailu odkazuje? Klikněte pravým (NIKOLI LEVÝM) tlačítkem myši na odkaz a z menu vyberte „kopírovat adresu odkazu“. Tu následně zkopírujte např. do poznámkového bloku a uvidíte, kam vede skutečný odkaz. Pozor dejte také na zkrácené odkazy, které maskují ten skutečný.

Nezaměňujte pracovní počítač za soukromý

Vědomí, že připojení k internetu při práci z domova neprobíhá zpravidla prostřednictvím připojení poskytovaného zaměstnavatelem, může svést ke zmenšené obezřetnosti při používání internetu na služebním zařízení. Zaměstnanec se tak může dostat i na stránky, které se typicky vyznačují zvýšeným výskytem různých škodlivých programů a na které by v rámci internetové sítě zaměstnavatele nikdy nepřistupoval. To může vést k zanesení škodlivého programu do „čistého“ zařízení, což následně může být velké riziko jak pro

samotné zařízení a informace na něm uložené, tak i pro informační systém organizace po opětovném připojení takového zařízení. Stejně je nutná zvýšená obezřetnost v případě, kdy je soukromý počítač využíván pro vzdálený přístup do informačního systému zaměstnavatele. Pokud používáte notebook nebo jiné zařízení zaměstnavatele, nikdy neinstalujte žádný podezřelý nebo nelicencovaný software.

Vyhněte se veřejným Wi-Fi sítím
Přes Wi-Fi sítě na veřejných místech nelze bez dalších zvláštních opatření přenášet osobní údaje a další citlivé informace. Bezpečnější je přenos prostřednictvím mobilních dat, případně použití VPN, tam kde to nastavení na součásti UK umožňuje. Hodláte-li využít VPN služby třetí strany, ověřte si reputaci provozovatele, sídlo a na základě jakých právních předpisů je služba provozována.

Přistupujte zodpovědně k volbě hesel
Nepoužívejte stejná hesla doma a v práci. Toto doporučení platí dvojnásob v případě údajů, pomocí kterých se přihlašujete do práce vzdáleně. V případě úspěšného útoku na domácí počítač je většinou snadné z prohlížečů a e-mailových klientů získat uložené přihlašovací údaje. Útočník by neměl být schopen přihlásit se pomocí hesla soukromého e-mailu také k tomu pracovnímu, případně někam dále.

Nepovolujte makra v běžných dokumentech
Většina kryptovirů používá v rámci svého šíření podvodné e-maily s dokumentem v příloze. Ten obsahuje výzvu k povolení aktivního obsahu a maker. Samotná příloha pak může vypadat např. jako sdělení, že dokument je napsán ve starší verzi textového editoru a bez povolení maker není možné skutečný obsah souboru zobrazit. Takovému požadavku nikdy nevyhovujte, následovalo by stažení a instalace škodlivého kódu. Nové verze kancelářských programů umějí pracovat i se staršími verzemi dokumentů a není třeba nic instalovat ani povolovat.

Nepodceňujte fyzickou bezpečnost počítačů
Počítač by měl po zapnutí vyžadovat ověření např. pomocí zadání hesla nebo biometrické autentizace. Následky případné krádeže můžete výrazně zmírnit zapnutím šifrování pevného disku. U většiny počítačů lze tuto funkci zdarma zapnout či doinstalovat, dopad na výkon je zanedbatelný. Šifrování výrazně snižuje riziko při ztrátě zařízení.

Dodržujte další praktická bezpečnostní opatření
Opatření mají být přiměřená míře rizika. Mezi důležitá opatření patří i adekvátní zabezpečení přístupu k zařízení (jeho obsahu) dalším členům rodiny. Zejména to platí pro děti, které mohou být i nevědomou příčinou vzniku některých rizik v tomto dokumentu.

Kdy kontaktovat Vaši lokální IT podporu?
- Na disku jsou místo Vašich běžných dokumentů soubory s neznámými příponami.
- Na disku jsou nové soubory, obsahující informace o zpřístupnění souborů po zaplacení výkupného. Většinou obsahují v názvu a obsahu souboru slova jako decrypt, recover, ransom atd.
- Došlo ke změně tapety na ploše nebo zobrazení oznámení přímo na obrazovce.
- V dalších případech, pokud pojmete podezření na nestandardní chování zařízení.

Kdy hlásit bezpečnostní incident?

Upozorňujeme na povinnost nahlásit pověřenci pro ochranu osobních údajů každý možný bezpečnostní incident. Jeho nahlášení je povinností každého pracovníka, nebo jeho nadřízeného, který zjistí některou z následujících skutečností:

- Bylo ztraceno nebo zcizeno zařízení nebo dokument, které obsahovalo soubor osobních údajů;
- byl neoprávněné osobě umožněn přístup k osobním údajům v zařízení nebo v dokumentu;
- osobní údaje v jakékoli formě byly umístěny bez přiměřené ochrany přístupu na místě, kde se k nim mohl neoprávněně někdo dostat;
- osobní údaje byly poškozeny nebo ztraceny;
- osobní údaje mohly být změny nebo upraveny, ale není možné ověřit, zda se tak stalo.

Ztrátu je třeba hlásit na adresu gdpr@cuni.cz. Dále viz: https://cuni.cz/UK-9092.html

Doporučení pro zaměstnavatele

- **Nepodceňujte zálohy a jejich ochranu**
- **Připravte konkrétní postupy pro rychlou reakci**
- **Vyhodnoťte a ohlaste porušení zabezpečení**

Nepodceňujte zálohy a jejich ochranu

V případě zašifrování významného množství dat v síti je třeba v první řadě ochránit zálohy. Je-li zálohování realizováno prostřednictvím kopírování souborů do jiné lokality v pravidelných časových intervalech, mělo by být možné automatické provádění záloh nouzově vypnout i bez zásahu správce. Ten nemusí být vždy k zastižení a případné „propsání“ viru do záloh může mít zásadní dopad. Lze tak důrazně doporučit zálohování implementovat způsobem, který umožňuje návrat k předchozím verzím souborů (např. pomocí tzv. inkrementálních záloh). Na to je nezbytné myslet již při návrhu či aktualizaci parametrů informační sítě součásti, jelikož pokročilé ransomware již útočí i na zálohy.

Připravte konkrétní postupy pro rychlou reakci

Začne-li kryptovirus šifrovat data, je třeba postižený počítač co nejdříve vypnout a informovat správce sítě o probíhajícím útoku. V těchto případech je důležitá každá minuta, čím méně škod stihne virus napáchat, tím lépe. Spolu se správcem by měl být ideálně informován i pověřenec pro ochranu osobních údajů, či další osoby, které jsou odpovědné za tzv. compliance (např. komunikaci se státními orgány). Konkrétní postupy by měly být součástí vnitřní dokumentace pro řešení bezpečnostních incidentů.

Vyhodnoťte a ohlaste porušení zabezpečení

Jestliže dojde k porušení zabezpečení osobních údajů, ať již na pracovišti, nebo v rámci práce z domova, které bude vyhodnocené jako rizikové pro práva a svobody subjektů údajů, vzniká Univerzitě Karlově povinnost toto porušení ohlásit Úřadu pro ochranu osobních údajů. Pokud se však podaří zastavit případný útok včas (nedošlo ke kompromitaci osobních údajů tím, že by se jich útočník zároveň zmocnil, a data byla obnovena ze zálohy), není zpravidla takový útok nutné ohlašovat, jelikož nenaplňuje podmínku rizika pro práva svobody subjektů údajů. I v takovém případě by však mělo dojít k zaznamenání incidentu ve smyslu čl. 33 odst. 5 obecného nařízení GDPR.