Základy kybernetické bezpečnosti

Přihlašovací údaje

Přestože je zabezpečení dat na síťových a cloudových úložištích na vysoké úrovni, nejslabším článkem obvykle bývá koncový uživatel, respektive způsob jeho autentizace: Pokud pro přístup používáte slabé heslo / heslo sdílené s jinými službami apod. a zároveň je heslo jediným prvkem autentizace, pak může vyzrazení hesla nepovolané osobě vést ke kompromitaci zabezpečení všech dat a služeb, ke kterým máte přístup.

Přístupové údaje k pracovním datům byste nikdy neměli zadávat do cizích počítačů (v kavárně, u kamaráda apod.), u kterých nemáte žádné povědomí ani záruky o jejich zabezpečení. Používejte svoje notebooky, telefony apod.

Abyste zvládli používat silná hesla unikátní pro každou službu, může být užitečné používat **kvalitní správce hesel**.

Soukromé počítače využívané pro pracovní účely

Je nutné si uvědomit, že na domácí počítače či jiná zařízení používaná pro přístup k pracovním datům by měly být kladeny stejné požadavky na zabezpečení jako na pracovní počítače. Málokdo má doma kamerový systém a vrátnici s nepřetržitým dohledem, proto věnujte **zvýšenou pozornost fyzickému zabezpečení v době vaší nepřítomnosti** (např. když jste na pracovišti).

Nezapomínejte na své ratolesti, které nejen mohou zapomenout zamknout při odchodu z domácnosti, ale často budou domácí počítač využívat spolu s vámi – striktní **oddělení uživatelských účtů na počítači pro pracovní a osobní účely** a nedostupnost administrátorských oprávnění dětem na sdíleném počítači by mělo být samozřejmostí. Stejně jako instalace **kvalitního antivirového a antimalware software a firewallu**.

Zabraňte instalaci her a podezřelého softwaru na počítač, který používáte k práci. **Instalujte jen důvěryhodný software**, u kterého jste ověřili jeho autenticitu, zamyslete se nad konfigurací softwaru (např. antivirové programy často automaticky odesílají soubory, které se jim zdají podezřelé, svému výrobci – takto mohou být z vašeho počítače bez vašeho vědomí odeslána data, která by se do rukou třetí strany dostat neměla).

Pamatujte, že data, která na domácím počítači nemáte, tam nemusíte chránit – ponechávejte pracovní data na síťových a cloudových úložištích a **na domácí počítač stahujete jen minimum dat a jen na nezbytně nutnou dobu**. Diskrétní a citlivá data pokud možno vždy šifrujte.

Povinnost hlášení ztráty služebních zařízení

Na základě pokynu pověřence na ochranu osobních údajů máte **povinnost nahlásit pověřenci každou ztrátu či odcizení každého zařízení nebo datového nosiče**, které mohou umožnit přístup k osobním nebo citlivým údajům, za které UK odpovídá. Tento pokyn se týká každého zařízení, ze kterého lze data získat např. prolomením ochrany (hesla) nebo vyndáním disku a získáním údajů samotných nebo hesel pro přístup do systémů univerzity. Typicky jde o notebook, tablet, počítač z kanceláře nebo i mobilní telefon s přístupovými údaji. Ztrátu co nejdříve oznámí pracovník, který ji zjistil, nebo jeho nadřízený, a to na adresu gdpr@cuni.cz .

Hlášení bezpečnostních incidentů

Koordinaci **řešení bezpečnostních incidentů v univerzitní síti** zajišťuje již od roku 2015 **bezpečnostní tým počítačové sítě Univerzity Karlovy** CSIRT-CUNI . Hlášení bezpečnostních incidentů zasílejte dle návodu emailem na abuse@cuni.cz .