CENTRUM INFORMATIZACE
A VÝPOČETNÍ TECHNIKY
ZÁPADOČESKÉ
UNIVERZITY
V PLZNI

cesnet
fondrozvoje
BEZPEČNOST.ZCU.CZ

Bezpečnostní desatero

1 Když nevíš, zeptáš se.

V případě podezření na kybernetický útok, když obdržím pochybný e-mail nebo se počítač chová divně, kontaktuji uživatelskou podporu a domluvím se na dalším postupu. Řídím se pokyny odborníků.

2 Budeš se autentizovat a autorizovat.

Počítač mě sám nepozná, proto mu musím svou identitu prokázat například znalostí hesla k uživatelskému účtu (autentizace). V aplikacích, programech a informačních systémech často nemám oprávnění ke všem činnostem. Proto po autentizaci následuje autorizace, která stanoví, co smím a co ne.

3 Dáš si pozor, kam heslo zadáváš.

Přihlašovací údaje vyplňuji pouze do webové stránky, která je šifrovaná, tedy její adresa začíná https:// nebo je na jejím začátku ikona zámku. Je důležité, aby adresa stránky byla uvedena přesně; i podvodné stránky mohou používat šifrování.

4 K příchozí poště budeš zdravě podezíravý/á.

Elektronická pošta je často zneužívána k rozesílání spamů, hoaxů, phishingových nebo hromadných zpráv. Dávám si pozor na podezřelé e-maily, zvláště na ty, které obsahují přílohu nebo odkazy na stránky. Příloha může obsahovat škodlivý kód a odkazovaná stránka může být podvodná.

5 Nebudeš věřit všemu, co se na Internetu píše.

Na Internetu může zveřejňovat informace každý, i autor neznalý nebo záměrně manipulující. Proto si věrohodnost získávaných informací vždy ověřuji. V pracovním prostředí musím zacházet s informacemi uváženě; ne všechny údaje jsou určeny všem.

6 Důvěrné informace budeš šifrovat.

Šifrování dat zajišťuje, že si informaci nemůže přečíst každý, kdo ji získá, ale jen ten, kdo zná navíc dešifrovací klíč. Elektronický podpis potvrzuje, že podepsaná osoba je autorem nebo že s obsahem souhlasí. Zároveň potvrzuje, že obsah elektronicky podepsaného dokumentu se po podepsání už nezměnil.

7 Na Internetu nejsi anonymní.

Prohlížením stránek i používáním služeb na Internetu po sobě zanechávám množství stop. Další stopy vznikají dobrovolným zveřejňováním informací o sobě, zejména na sociálních sítích. Všechny tyto činnosti moji anonymitu snižují a je dobrým zvykem chovat se tak, jako by mě mohl kdokoli identifikovat.

8 Budeš chránit své počítače a data zálohovat.

Nikdo nepovolaný by neměl používat cizí osobní věc, jakou je například počítač. Takové zařízení musím chránit zamykáním kanceláře a používáním zámku obrazovky. Dbám na aktuálnost jeho programového vybavení, případně svěřím správu zařízení odborníkům. Důležitá data pravidelně zálohuji.

9 Mobilní zařízení jsou také počítače.

Mobilní zařízení, dnes nejčastěji chytrý mobilní telefon, je malý počítač a chovám se k němu a datům v něm stejně jako v případě počítače. Navíc si musím uvědomovat rizika, která přináší možnost zařízení přenášet nebo ho mít stále u sebe.

10 Budeš dodržovat pravidla a ctít právo.

Na Internetu platí stejná legislativa jako v reálném světě, ale je rozšířená o některé další specifické právní normy. Mimo tuto státem vyžadovanou legislativu dodržuji také interní pravidla organizací nebo pravidla používání konkrétních služeb.