Jak postupovat při podezření na bezpečností incident

Kybernetický incident může potkat každého – kliknutí na podvodný e-mail, ztracený notebook, neznámá aplikace, která se sama nainstalovala...
Důležité je **nepanikařit, ale jednat rozumně a včas**.

Co je bezpečnostní incident?

Za bezpečnostní incident považujeme každou událost, která může ohrozit bezpečnost vašeho účtu, zařízení nebo univerzitních dat.

Příklady
- ztráta nebo krádež zařízení (notebook, mobil, USB disk),
- podezřelý e-mail nebo zpráva, která se tváří jako komunikace z UK,
- zjištění, že jste se přihlásili na falešnou stránku CAS,
- neobvyklé chování počítače (sám odesílá e-maily, zpomaluje, otevírá reklamy),
- náhlé uzamčení souborů s požadavkem na výkupné,
- podezření, že váš účet používá někdo jiný.

Co udělat okamžitě?

Postup se může lišit podle typu problému – ne vždy je nutné dělat všechny kroky hned.

Pokud jste obdrželi podezřelý e-mail nebo zprávu
- na odkazy neklikejte a přílohy neotvírejte,
- e-mail přepošlete IT podpoře nebo bezpečnostnímu týmu k posouzení.

Pokud máte podezření, že je zařízení napadeno nebo ztraceno:
- pokud vás k tomu IT podpora nevyzve jinak, zařízení **odpojte od internetu** (Wi-Fi, kabel),
- nepokoušejte se problém řešit sami ani neinstalujte „čisticí“ nástroje,
- zařízení ponechte vypnuté nebo offline podle pokynů IT podpory.

Změňte heslo do CAS
Změňte si heslo do CAS zejména tehdy, pokud:
- jste se přihlásili na podezřelé nebo falešné stránky,
- máte podezření na zneužití účtu.

Použijte jiný, důvěryhodný počítač a zvolte nové, silné heslo, které nepoužíváte jinde.
Nahlaste incident IT podpoře fakulty nebo bezpečnostnímu týmu CSIRT-CUNI
- čím dříve incident nahlásíte , tím snáze se dá škoda omezit.
- pokud si nejste jistí, zda jde o incident, **raději se poraďte** – i podezření je důležité.

Nevyšetřujte problém sami
- neinstalujte žádné „čistící nástroje“ ani nestahujte podezřelý software,
- zařízení ponechte vypnuté nebo v režimu offline, dokud IT pracovník neprovede kontrolu.

Jak incident nahlásit?
Při hlášení poskytněte co nejvíce informací – pomůže to rychlejšímu vyřešení.
Podrobný postup najdete v sekci Hlášení bezpečnostního incidentu , kde se dozvíte, jak incident popsat, komu ho zaslat a jak probíhá řešení.
Pokud dojde ke ztrátě zařízení s osobními daty studentů či zaměstnanců, IT oddělení situaci dále hlásí **Úřadu pro ochranu osobních údajů**, jak ukládá legislativa.

Jak poznat, že šlo o incident?
Najednou se **nemůžete přihlásit** do univerzitního účtu.
Změnilo se heslo bez vašeho vědomí.
Z vašeho e-mailu **odchází zprávy, které jste nenapsali**.

Souborům zmizela přípona nebo se nedají otevřít.
Na obrazovce se objeví **žádost o výkupné nebo upozornění na „vir“**.
Raději **jednejte ihned** – i planý poplach je lepší než přehlédnutý útok.

Jak incidentům předcházet
Buďte obezřetní při práci s e-maily a přílohami.
Neinstalujte software z neznámých zdrojů.
Používejte silná hesla a dvoufaktorové ověření.
Pravidelně zálohujte důležitá data.
Aktualizujte systém i aplikace.

Často kladené dotazy (FAQ)
Mám nahlásit i e-mail, který „jen“ vypadal podezřele?
- Ano. I když jste na nic neklikli, pomůže to IT oddělení odhalit probíhající útoky a ochránit ostatní.

Klikl/a jsem na odkaz, ale nezadal/a jsem heslo – mám něco dělat?
- Pro jistotu incident nahlaste. Útočníci mohou i bez zadání hesla shromažďovat informace o zařízení nebo IP adrese.

Musím hlásit ztrátu notebooku se šifrovaným diskem?
- Ano. Přestože nemůže díky šifrování disku dojít k úniku citlivých dat, univerzita musí podle GDPR takové události evidovat.

Jak postupovat v 5 bodech při podezření na útok
3. Změňte heslo do CAS z jiného, důvěryhodného zařízení.

1. Zachovejte klid.
4. Nahlaste incident IT podpoře.

2. Odpojte zařízení od internetu (Wi-Fi, kabel, synchronizace s cloudem).
5. Nepokoušejte se problém řešit sami. Vyčkejte na pokyny IT oddělení.

***Pamatujte** : Rychlá reakce může ochránit nejen vás, ale i univerzitní systémy a data kolegů.*