

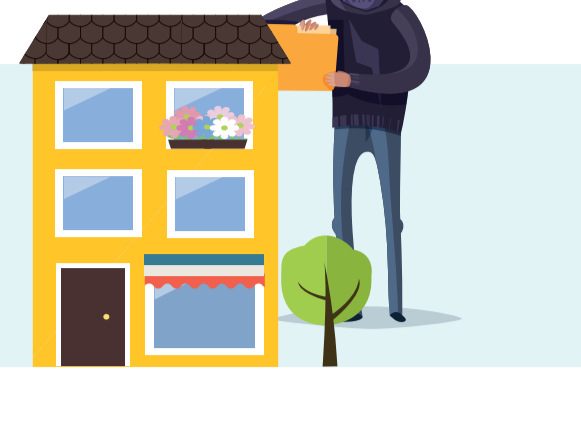
SURVIVAL GUIDE pro menší firmy

...aneb jak přežít v oblasti kybernetické bezpečnosti.



Dle výzkumu institutu Ponemon až 70 % kybernetických útoků cílí na malé a střední podniky.

70 %



Důvodem je časté podceňování zabezpečení z důvodu velikosti a neatraktivnosti firmy.



Na černém trhu se **nejčastěji vyskytují informace** o účtech, kreditních kartách nebo přístupech k internetovému bankovníctví.

Důsledky krádeží dat



- Firmy **nesou** za únik dat **odpovědnost**.
- **Některá data jsou chráněna zákony** a předpisy (v EU GDPR, v USA HIPAA a PCI).
- **Zaznamenávejte** postup, jak s důvěrnými daty nakládáte. Dokumentace vám poslouží jako důkazní prostředek v případě úniku dat.
- V některých případech **jsou firmy povinny hlásit únik dat** (např. při ztrátě USB disku s lékařskými záznamy).

Jak důsledně zabezpečit firemní infrastrukturu?



1. Posuďte svá aktiva, rizika a zdroje

60 %

zaměstnanců obchází bezpečnost pomocí mobilních zařízení.

48 %

zaměstnanců se pokusilo deaktivovat firemní bezpečnost.



Vytvořte seznam všech koncových stanic včetně mobilů.



Zkontrolujte online služby jako Salesforce, iCloud či Google Docs a zvažte rizika s nimi spojená.



Položte si otázku kdo nebo co je hrozba, vyhodnoťte rizika a případné škody, které mohou způsobit.



Užitečné informace najdete na stránkách Europolu nebo institucí CERT-EU a ENISA-EU.

2. Doporučujeme využít 3 základní technologie



Antivirový program

Brání škodlivému kódu vniknout do firemní infrastruktury.



Šifrovací nástroj

Šifruje veškerá důvěrná data.



Dvoufaktorová autentizace (2FA)

Jde o nezbytný prvek při zabezpečení dat a prevenci jejich úniků.



Dvoufaktorová autentizace přidává k uživatelskému jménu a heslu další vrstvu zabezpečení v podobě jednorázového hesla. Ověření nejčastěji probíhá pomocí kódu, skenu obličeje nebo otisku prstu.

3. Vzdělávejte!



Investice do povědomí zaměstnanců o bezpečnosti se vyplácí.



Vzdělávejte na všech úrovních od vedoucích pracovníků, prodejců i partnerů.

21 %

zaměstnanců otevřelo phishingový e-mail.

16 %

zaměstnanců dokonce otevřelo přílohu.

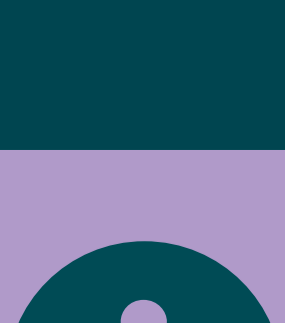
4. Vyhodnocujte, testujte a provádějte audit



Budování bezpečné IT infrastruktury není jednorázový projekt, ale dlouhodobý proces.



Zvažte služby externího konzultanta bezpečnosti a provádějte pravidelné penetrační testy a bezpečnostní audit.



Pokud chcete mít přehled o aktuálních hrozbách, **přihlaste se k odběru** na [webch eset.cz/blog](http://webch.eset.cz/blog), dvojklik.cz nebo welivesecurity.com.