JAK MINIMALIZOVAT DOPADY KYBERNETICKÝCH HROZEB

Plán řízení kybernetických rizik.

AUDIT

Je důležité podrobně popsat, jaká data vaše společnost shromažďuje, kde jsou tato data uložena (na kterém místě v síti nebo v cloudu) a kdo k nim má přístup. Z tohoto důvodu je prvním krokem při vývoji plánu řízení kybernetických rizik identifikace všech relevantních digitálních aktiv.

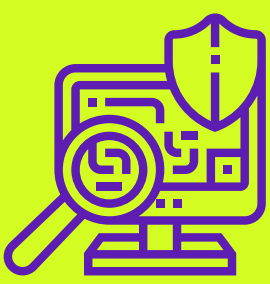
Audit by měl rovněž odhadnout náklady, které mohou vzniknout v případě porušení citlivých údajů.

POSOUZENÍ ZABEZPEČENÍ

Dalším krokem je analýza současných způsobů zabezpečení dat vaší organizace. Je důležité provést důkladné posouzení, jaké prvky vaší IT infrastruktury, ať už on-permise nebo v cloudu, mohou být nejvíce náchylné k interním či externím útokům. Nezapomínejte také na své zaměstnance či fyzické zabezpečení budov.

Cílem je odhalit případné nedostatky v aktuálním způsobu zabezpečení dat, aby je bylo možné odstranit.

KLASIFIKACE HROZEB



Na základě předchozí analýzy je třeba posoudit všechny zjištěné hrozby pro systémy, data i uživatele v celé vaší organizaci. Útočníci mohou chtít ukrást zákaznická data, narušit vaše obchodní operace nebo “jen” poškodit pověst vaší firmy. Někteří kyberzločinci požadují výkupné za to, že obnoví vaše data, nebo vaši společnost nezdiskreditují.

Seřaďte tedy hrozby dle závažnosti a postupně se soustřeďte na jejich eliminaci.

PLÁN ZOTAVENÍ PO HAVÁRII

To nejdůležitější na konec. Váš plán řízení kybernetických rizik musí podrobně popsat, co bude následovat v případě narušení nebo ztráty dat. To znamená, že musíte mít připraven plán na zotavení po havárii a to jak pro vaše data a tak i IT infrastrukturu a konkrétní pokyny pro jednotlivé zaměstnance.

Cílem této části dokumentu je poskytnout svým zaměstnancům pokyny a postupy, jak co nejrychleji po útoku vrátit chod společnosti do normálu.

VÍCE SE DOZVÍTE NA HTTPS://BOIT.CZ