TŘI ÚDAJE O HESLECH, KTERÉ BY VÁS MĚLY ZAJÍMAT

Za drtivou většinou hackerských útoků a úniků dat, které mohou zdiskreditovat či zlikvidovat vaší společnost stojí slabé heslo, které nějakým způsobem uniklo. Způsobů úniků je mnoho, tak zmiňujeme jen ty nejčastější.

65 % útoků je způsobeno díky úspěšnému cílenému phishingu, sociální inženýrství je úspěšné v 79 %. 94 % malware bylo do sítí doručeno pomocí e-mailů. 90 % zaměstnanců využívá firemní zařízení k soukromým účelům.

TŘI ALARMUJÍCÍ UKAZATELE

51 %

Tolik uživatelů používá obvykle 5 stejných hesel pro přístup k soukromým i firemním účtům.

69 %

Je poměr uživatelů, kteří sdílejí se svými kolegy stejné heslo do některého z firemních systémů.

81 %

Celkový počet úniků dat, kde vyšetřování prokázalo, že bylo zaviněno díky uniklému či slabému heslu.

JAK SE VYHNOUT PROBLÉMŮM

Školte své uživatele

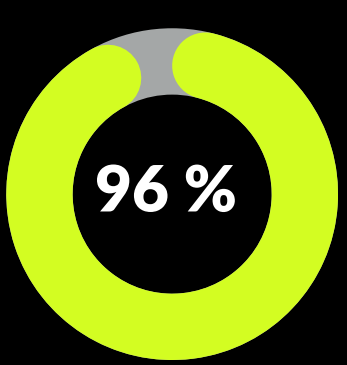
Útočníci využívají malware, sociální inženýrství a phishing aby z uživatelů vylákali hesla.

Proveďte audit bezpečnosti

Udělejte si bezpečnostní audit, odhalte slabé stránky vašeho zabezpečení a zapracujte na nich.

Nastavte bezpečnostní politiky

Vynuťte vyšší bezpečnostní politiky pro všechny uživatele a centrálně je spravujte a monitorujte.



Až 96 % uživatelů, kteří byli proškoleni, mají šanci odhalit cílený phishing či další formy podvodu.