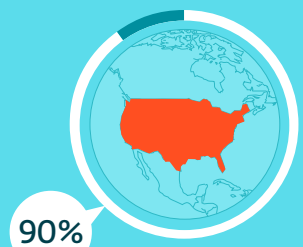
Zabezpečení firemních dat

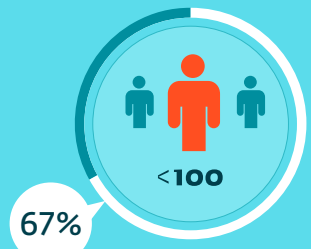
MALÉ A STŘEDNÍ FIRMY*

Snadný cíl kybermafie

SMB většinou nejsou primárním cílem útočníka, ale díky v praxi často uvolněným bezpečnostním politikám, může jít o cíl velmi snadno dosažitelný.

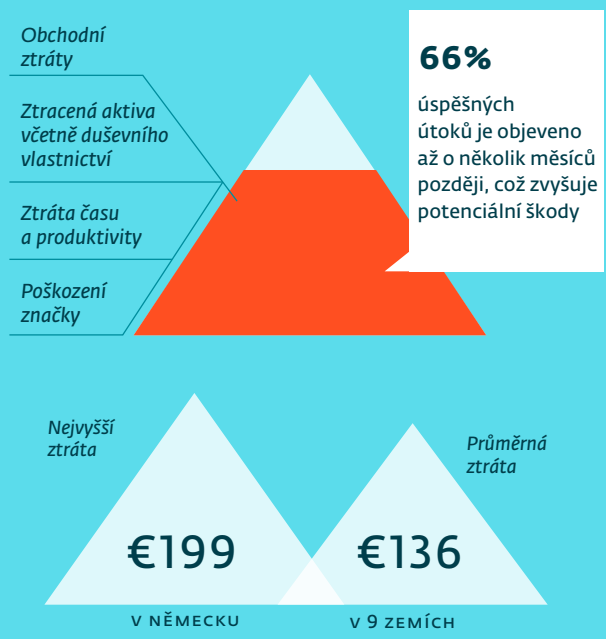


90% firem v USA bylo v minulém roce vystaveno různým formám kyber útoků



67% útoků cílilo na menší organizace *(méně než 100 zaměstnanců)*

Reálné náklady narušení bezpečnosti



* ZDROJ: Verizon Data Breach Report 2013

SLABÁ HESLA

#1 Největší bezpečnostní riziko: ukradení hesel

61% UŽIVATELŮ POUŽÍVÁ JEDNO HESLO PRO VÍCE ÚČTŮ

76% ÚTOKU ZNEUŽÍVÁ SLABÉ NEBO UKRADENÉ PŘIHLAŠOVACÍ ÚDAJE

44% UŽIVATELŮ MĚNÍ HESLO JEDNOU ROČNĚ

Tipy pro silnější heslo

str0ngPassSTOPhack3rs!*

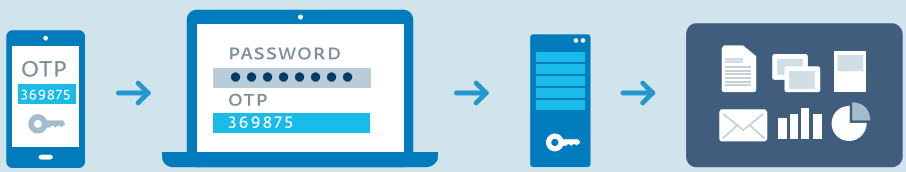
- Kombinujte velká a malá písmena, číslice a symboly
- Používejte více než 8 znaků (kombinace slov, 20 – 30 znaků)
- Měňte hesla častěji než jednou ročně

abc123	*Čísla na konci hlavně číslice 1 nebo 2*
Abcd	*Velká písmena na začátku*
John123	*Křestní jména (obvyklé u žen)*
golf123	*Zájmy (obvykle u mužů)*

HACKEŘI BEZ ŠANCE

při dvoufaktorové autentizaci (2FA)

2FA ověřuje identitu uživatele a chrání citlivá data



SMARTPHONE S JEDNORÁZOVÝM HESLEM

UŽIVATELSKÉ HESLO KOMBINOVANÉ S JEDNORÁZOVÝM

AUTENTIZAČNÍ SERVER

FIREMNÍ DATA

Tato infografikau vytvořil ESET – výrobce bezpečnostních řešení. Více informací o 2FA – produktu **ESET Secure Authentication** – *na www.eset.cz*

ENJOY SAFER TECHNOLOGY™

Zdroje:
Verizon Data Breach Report 2011-13
Ponemon Institute: 2013 Cost of Data Breach Study: Global Analysis
2013 Information Security Breaches Survey: The Department for Business, Innovation and Skills (BIS) and PWC
CSID Customer Survey: Password Habits 2012