

zapomínejte na bezpečnost

Prve začíná, může mít větší sklon ignorovat hrozby v naději, že nepředstavuje speciální útočníky dostatečně lákavý terč. Vše zakládané firmy a živnosti platí všechny IT bezpečnosti – úplně stejně, jako platí kdo podnikají již dlouho.

Autorem: Miroslav Václavík

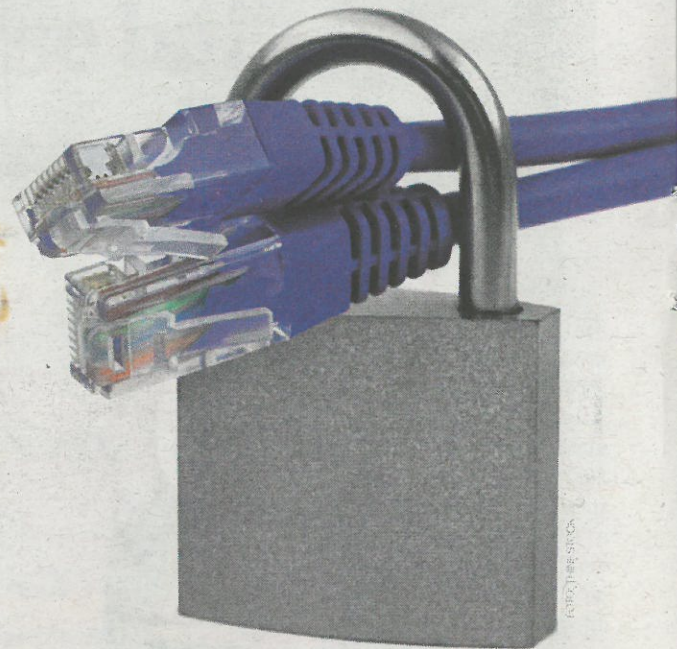
Argumentace o ignorování IT hrozeb je však lišná, a to ze dvou hlavních důvodů: na 70 % z hlediska IT útoků „civilní obětí“ jsou subjekty, než na které útok cílil. V závěru vyšetřování analyzovaných případů v rámci Investigativní společnosti byl hlavním důvodem pro přístup k IT je, že útočníci

v řadě případů nerozlišují mezi velkými a malými firmami. Příkladem útoku, který průběžně, bez ohledu na velikost firmy nebo délku její tradice, je útok vyděračského šifrovacího malware, kdy vyděrači zašifrují soubory na počítači a požadují výkupné za dešifrovací klíče.

Příkladem byla rozsáhlá kampaň vyděračského malware (tzv. ransomware) TorrentLocker. Zloincům se podařilo infikovat na 40 tisíc počítačů, převážně v Evropě. Malware Torrent-

Locker zašifroval na těchto počítačích (resp. na všech jejich připojených diskových jednotkách) přes 525 milionů souborů, za jejichž dešifrování požaduje gang vyděračů výkupné. V průměru je to přes 2,5 bit-coinu, tedy téměř 25 tisíc korun. Výkupné zaplatilo pouze 570 obětí, ale i tak si vyděrači přišli na 585 tisíc dolarů.

V Česku se obětí TorrentLockeru stalo 3420 počítačů, na nichž bylo zašifrováno 35 milionů souborů. Vyděračům zaplatilo 28 obětí



z Česka a to celkem v počtu 611 tisíc korun.

Online vydírání

Kampaň představuje jen malou část expanze ransomware. Dá se očekávat, že podobných kampaní bude přibývat. Vyplývá to alespoň ze závěrů panelu expertů na prestižní konferenci právnícké fakulty americké Georgetown University "Cybercrime 2020: The Future of Online Crime and Investigations", která se konala v prosinci 2014. Podle tohoto

panelu představuje vydírání pomocí malware budoucnost online kriminality.

Vyděračský malware není jedinou hrozbou, jíž podniky a podnikatelé čelí. Je proto důležité mít na všech počítačích, tabletech a smartphonech nainstalované bezpečnostní řešení, chránit přístup k systémům a datům pomocí dvoufaktorové autentizace, chránit data šifrováním a používat kvalitní řešení pro zálohování dat a jejich obnovu v případě havárie. ■

DOKAŽTE VÍCE
BEZPEČNOSTNÍM ŘEŠENÍM ESET

At už jste majitel společnosti, nebo se jen staráte o firemní IT, bezpečnostní produkty ESET jsou rychlé, jednoduše se používají a mají skvělou technologii detekce škodlivého kódu. Přinášíme úroveň ochrany, díky které můžete pracovat efektivněji.
Více informací na: eset.cz/firmy,
tel.: 222 811 100, e-mail: obchod@eset.cz

BAGETERIE BOULEVARD

Stanislav Novotný:
**„Chcete vlastní franšizu?
Já už ji mám!“**

Již od 5 000 000 Kč vlastních prostředků
BAGETERIE BOULEVARD je zavedená česká značka s více jak 12letou historií úspěšného fungování. Vzhledem k tomu, že stále cítíme svůj potenciál růstu v rámci České republiky, plánujeme otevírání dalších poboček. Máte-li zájem o spolupráci, objednejte se k nám na nezávazný pohovor, kde Vám sdělíme více.

bb.cz bb-fransiza.cz

www.bibbyfinancialservices.cz

PODNIKEJTE S JISTOTOU

Provozní financování od Bibby Financial Services

Volejte: **800 111 008**

BIBBY
FINANCIAL SERVICES
Moving business forward

INFOpower
modulární ERP systém
pro řízení stavebních firem

Efektivní řízení nákladů stavebních zakázek
Rychlé a flexibilní plánování kapacit a zdrojů
Řízená správa obchodních dokumentů
Přehledné manažerské výstupy

Svět stavebnictví na dotek **RTS**

RTS a. s., Lazaretní 13, Brno 615 00, www.rts.cz
e: rts@rts.cz, t: +420 545 120 211, f: +420 545 120 210