Vážené čtenářky, vážení čtenáři,

tématem posledních týdnů jsou bezesporu problémy, které vznikly kvůli koronavirové nákaze. Rizika hrozí nejen kvůli tomu, že se velká část kancelářských zaměstnanců přesunula do svých domácích pracoven, ale že současně i hackeři výrazně zvýšili svou nekalou činnost.

Rizika jsou tak vyšší v mnoha oblastech, jako jsou servery přímo přístupné z internetu, webové stránky a jejich formuláře, certifikáty, aplikace a komponenty třetích stran nebo mobilní řešení. I když některé z těchto hrozeb mohou být dočasné, mnoho z nich tu pravděpodobně přetrvá, a pro bezpečnostní týmy to bude představovat novou výzvu.

Velké změny se dají očekávat právě v oblasti práce z domova. Podle nedávné studie Gartneru firmy předpokládají, že se trvale přesune do domácích kanceláří až 5 % odpovídajících zaměstnanců.

Podobný průzkum u nás minulý měsíc vykonal Median a podle něj zhruba dvě třetiny tuzemských oprávněných zaměstnanců by uvítaly do budoucna nějakou formu práce z domova, přičemž každý desátý by dokonce chtěl výhradně pracovat na dálku.

Rizikům ale čelí i cloudové služby, jejichž využívání se podle McAfee v posledních měsících i díky práci z domova zvýšilo až o polovinu, v případě videokonferenčních systémů dokonce o více než 600 %. Počet útoků na cloudové účty (především šlo o platformy pro týmovou spolupráci jako třeba Microsoft 365) se přitom ve stejném období zvýšil o neuvěřitelných 630 %.

Největší nárůst hrozeb zaznamenaly dopravní a logistické, vzdělávací a vládní instituce, a to i o více než 1 000 %, následovaly výroba s téměř 700 %, finanční služby se zhruba 600 % a energetické společnosti se zvýšením ohrožení o téměř 500 %.

To vše ale nekoresponduje s tím, jak se chovají samotní uživatelé, kteří si naopak chtějí práci z domova především co nejvíce ulehčit, a proto často dbají na bezpečnostní zásady méně, než by to dělali v práci, včetně například nutnosti využívat VPN připojení nebo vícefaktorovou autentizaci.

V nejnovějším Security Worldu vám přinášíme spoustu rad, jak ve firmě práci z domova podpořit co nejbezpečnějším způsobem, jak se spolehlivě chránit při videokonferenčních mítincích či jak využívat řešení pro týmovou spolupráci, aniž to ohrozí citlivé informace podniku, s nimiž uživatelé doma zákonitě pracují.

Teď o prázdninách tak můžete zvážit všechny možnosti, jak se nové situaci přizpůsobit a jak se stát nejen bezpečnější organizací, ale i atraktivnějším místem pro své zaměstnance.

S přáním příjemně stráveného léta někde u vody či na horách

Pavel Louda
vedoucí projektu

Obsah