

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **83** ze dne **17.9.2024**

5 nejčastějších chyb a problémů v zabezpečení IT u menších firem

Společnost GFI Software sestavila přehled pěti nejčastějších bezpečnostních mezer, které nachází u menších firem a organizací. Ty se z hlediska kybernetické bezpečnosti dopouštějí celé řady vážných chyb, jako je nezáplatovaný software, otevřené porty či nedostatečné zabezpečení mobilních zařízení. Související problémy pak většinou řeší manuálně a s pomocí neúplných nástrojů, což značně zatěžuje firemní zdroje. Postupují jako zahradník, který zanedbá ošetření proti plevelům a pak se na ně vrhá s motykou.

Pokud se podíváme na běžné chyby a problémy v zajištění kybernetické bezpečnosti malých a středních společností (SMB) v oblasti zranitelností, tak nejčastěji se zde setkáme s:

1. Nezáplatované operační systémy a software – Pokud se objeví nenápadné oznámení "aktualizace je k dispozici", uživatelé obvykle kliknou na "Připomenout později". Tyto aktualizace se netýkají jen nových funkcí, často se jedná o zásadní bezpečnostní záplaty, které brání v neautorizovanému přístupu. SMB podniky ale většinou nemají nástroj, který automaticky skenuje síť a hledá chybějící aktualizace operačních systémů, webových prohlížečů a softwaru třetích stran, a případně je dokáže centrálně nasadit.
2. Otevřené porty a chybně nakonfigurované služby – Otevřené porty a špatně nakonfigurované služby jsou jako odemčené dveře do firemní sítě. Jsou to snadné vstupní body pro lidi, kteří hledají příležitost k průniku do sítě. Aby se tak nestalo, je třeba kontrolovat otevřené porty, zkoumat sdílené adresáře. Současná databáze popisuje 60 000 známých problémů, a všechny sledovat rozhodně nelze manuálním způsobem.
3. Nedostatečná viditelnost sítě – Nelze chránit to, co není vidět. Pokud administrátor neví, co všechno je připojeno k síti, nemůže ji spolehlivě zabezpečit. Proto je důležité nejdříve zjistit a katalogizovat každé zařízení v síti – počítače, telefony, tiskárny, servery a další. Tento komplexní soupis vytváří jasný a podrobný obraz celého digitálního ekosystému. Teprve pak má organizace jistotu, že má všechna zařízení pod kontrolou a zabezpečená.
4. Slabé zabezpečení mobilních zařízení – Dříve se na pracovišti využívaly jen firemní počítače, tiskárny a další zařízení. Nyní, když všichni používají k práci i telefony a tablety, podniková síť sahá daleko za zdi kanceláře, což vytváří spoustu potenciálních slabých míst. Je proto potřeba tato zařízení izolovat nebo je zabezpečit stejně jako kancelářské počítače – ať již se jedná o firemní telefon nebo osobní tablet používaný k práci.
5. Mezery v dodržování zákonných předpisů – Udržet soulad se zákonnými předpisy, ať již s těmi všeobecnými či specifickými pro konkrétní odvětví, může být opravdový oříšek. Většina z nich vyžaduje generování bezpečnostních reportů prokazujících dodržování požadovaných pravidel, což bez těch správných nástrojů může být nespílitelný úkol.

"Rozšiřující se IT infrastruktury znamenají pro mnoho SMB firem dramatický nárůst zranitelností jejich sítí a s tím spojených bezpečnostních hrozeb," řekl Jozef Kačala, Vicepresident of Global Sales Engineering ve společnosti GFI Software. "Mnohé organizace se snaží těmto výzvám čelit s pomocí freewaru nebo neúplných nástrojů, které neřeší situaci komplexně ale pouze částečně. Ucelené nástroje typu GFI LanGuard nabízejí komplexní a centralizovaný přehled o mezerách a zabezpečení lokálních sítí s využitím širokých možností

MEATEST spol. s r.o. - sdělení pověřence pro ochranu osobních údajů číslo **83** ze dne **17.9.2024**

automatizace a umělé inteligence (AI)."

Zdroj: AVcentrum ČR