

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **5** ze dne **8.2.2022**

Čtvrtina evropských firem podceňuje investice do IT bezpečnosti. Osm z deseti přitom již bylo napadeno.

Každý desátý útok, který byl loni ve firmách zablokovan, mohl podle expertů způsobit vážné narušení bezpečnosti. Přesto z nedávného průzkumu vyplývá, že 23 % manažerů evropských firem ví o tom, že jejich společnost nevynakládá dostatečné prostředky na prevenci před kybernetickými útoky. Vzhledem k tomu, že takřka osm z deseti (79 %) evropských firem se někdy stalo obětí takového útoku, měli by odpovědní manažeři posílit ochranu a používat nejmodernější technologie k ochranu majetku a úspore nákladů, které by bylo nutné vynaložit při narušení firemní bezpečnosti.

Kybernetické útoky cílené na firmy všech velikostí jsou stále nebezpečnější hrozbou a dělají vrásky na čele manažerům po celé Evropě. K dispozici jsou přitom sofistikovaná řešení, která jim mohou pomoci ochránit firemní majetek nebo alespoň snížit finanční dopady v případě, že by byl útok úspěšný. Paralelně s vývojem kybernetických hrozeb se totiž vyvíjejí i bezpečnostní řešení a služby, které mají nesporný přínos pro všechny uživatele. Přesto zpráva *"Must-have cybersecurity insights for proactive business decisionmakers"* prokázala, že firmy a jejich vedoucí manažeři nedělají dost pro to, aby byli dostatečně ochráněni, protože nevědí jak.

Malware, nezkušený personál a chybějící ochrana: neuralgické body, které nedávají manažerům spát

63 % z 1 500 dotazovaných manažerů uvedlo, že se obávají kybernetických útoků, a to zejména následujících typů:

- Spyware: 64 %
- Ransomware: 63 %
- Malware: 63 %
- Cílený útok (na organizaci nebo obor): 63 %
- E-mail: 62 %

Více než polovina (53 %) manažerů se také obává, že zaměstnanci nedodržují bezpečnostní zásady a postupy. Pouze pětina (21 %) těmto schopnostem zaměstnanců naopak plně důvěřuje. Podle 64 % respondentů je sledování možných rizik nebo narušení bezpečnosti komplikovanější kvůli výrazně častějšímu používání osobních zařízení a cloudových služeb zaměstnanci při práci z domova.

"Náš průzkum jasně ukazuje, jaké problémy musí firmy bez ohledu na svoji velikost řešit, ať už se jedná o chyby zaměstnanců, e-mailové útoky nebo rostoucí složitost IT infrastruktury. Pomoc nabízejí sofistikovaná bezpečnostní řešení, která nabízejí více než jen ochranu koncových bodů, lepší informace o hrozbách a budování bezpečnostního povědomí zaměstnanců. Ideální je vybrat si služby jednoho partnera z oblasti kybernetické bezpečnosti, který nabízí jak technologii, tak odborné znalosti, abyste získali komplexní ochranu a měli přehled o všem, co se ve vaší síti děje. Firmy tak dokážou lépe reagovat na současné i budoucí kybernetické hrozby," říká Miroslav Kořen, generální ředitel společnosti Kaspersky pro region východní Evropy.

Zpráva prokazuje, že investice do externího zabezpečení IT se vyplatí a pomáhají předcházet závažným incidentům. Průzkum zjistil, že firmy, které si kybernetickou bezpečnost zajišťují externě, čelily téměř o 10 % menšímu počtu kybernetických incidentů než firmy, které se spoléhaly pouze na interní zdroje. V roce 2021 se proto firmy začaly více zajímat o externí pomoc. Další průzkum zjistil, že firmy všech velikostí se stále častěji obracejí na poskytovatele spravovaných služeb (MSP), aby si zajistily lepší ochranu v náročném prostředí.

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **5** ze dne **8.2.2022**

Rychlé zavádění nových technologií, nové pracovní postupy a stále větší složitost infrastruktury přiměly firmy k tomu, aby řešení bezpečnosti svěřily vysoce kvalifikovaným odborníkům mimo svoji organizaci.

Doporučení pro firemní manažery

Firmy mohou zvýšit úroveň zabezpečení pomocí integrace SOC (Security Integration Center) a SIEM (Security Information and Event Management). Pro malé a střední podniky je nejjednodušším způsobem, jak čelit současným výzvám v oblasti zabezpečení IT, využití důvěryhodné externí odborné pomoci. V této souvislosti navrhují odborníci manažerům firem několik následujících opatření:

- S obranou proti závažným hrozbám mohou pomoci specializované služby.
- Používejte specializovanou sadu nástrojů pro účinnou ochranu koncových bodů, detekci hrozeb a reakci na ně, abyste včas odhalili a odstranili i nové a skrývající se hrozby.
- Zajistěte svému bezpečnostnímu týmu přístup k nejnovějším informacím o hrozbách a dbejte na průběžné zvyšování jeho kvalifikace pomocí odborných školení.
- Zajistěte svým zaměstnancům základní školení o kybernetické bezpečnosti, protože mnoho cílených útoků začíná phishingem nebo jinými technikami sociálního inženýrství.
- Důležitá je integrace odborných znalostí a technologií. Pokud získáte obojí od jednoho důvěryhodného partnera, který poskytuje integrované a alespoň částečně automatizované služby, budete mít přehled o veškerém dění ve firemní síti, ušetříte čas a zvýšíte efektivitu. Váš bezpečnostní tým se pak bude moci věnovat důležitějším záležitostem.

zdroj: Avcentrum ČR