accenture

TRENDY V OCHRANĚ PŘED KYBERÚTOKY

VIDEO TRANSCRIPT

Název videa:
Trendy v ochraně před kyberútoky

Před pěti lety u nás v České republice vzniklo unikátní expertní centrum Cyber Fusion Center, ve kterém pracují experti z více než 30-ti národností s odlišným zaměřením. Ti poskytují služby v oblasti kyberbezpečnosti klientům z po celém světa.

Simulujeme reálné útoky na aplikace, infrastrukturu, stroje, nebo celou společnost za využití propracovaných scénářů. Klientům tak pomáháme objevit slabá místa jejich zabezpečení a navrhujeme řešení všech nedostatků.

Kromě ochrany proti útokům pomáháme i se správou privilegovaných účtů, nebo třeba se zabezpečením cloudu. Máme vlastní 24/7 dozorové centrum, které okamžitě detekuje a reaguje na incidenty ohrožující bezpečnost klientů.

Předcházení útokům

Naším prvotním úkolem je přesvědčit vás i všechny ostatní, že kyberbezpečnost je nutné vnímat jako nedílnou součást byznysu. Stejně důležitou, jako je třeba účetní oddělení.

Klientům, kteří si to neuvědomují, je těžké pomoci, protože jsou to primárně oni, kdo jsou zodpovědní za bezpečné nakládání s daty svých zaměstnanců a zákazníků. My jim k tomu poskytneme nástroje a odborné poradenství.

Ať už se klient rozhodne své zabezpečení outsourcovat, nebo si postavit vlastní bezpečnostní tým, v obou případech je Accenture připravena dodat end-to-end řešení. Jsou i případy, kdy poskytujeme služby kontrolního mechanismu, který udržuje aktivitu zabezpečení na straně klienta neustále v pozoru. A je jedno jestli se jedná o klienty z oblasti průmyslové výroby, nebo banky.

Klient si musí sám stanovit, co pro něj bezpečnost znamená a jak je potřeba ji nastavit, aby byl jeho byznys bezpečný, odolný a připravený na možné kyberútoky. V tomto směru umíme velmi dobře poradit, protože v rámci Accenture sledujeme trendy ve všech odvětvích napříč kontinenty.

Máme vlastní Threat Intelligence tým, takovou tajnou službu v komerčním online světě. Týmy zkušených analytiků sledují probíhající útoky, mají přehled o tom co se prodává na různých „darknet“ serverech a podle toho vyhodnocují a následně s námi sdíli potenciální hrozby a cíle hackerských útoků.

Klient tak díky nám získává konkurenční výhodu a je o krok napřed. Predikce možného útoku je velmi důležitá pro odpovídající nastavení bezpečnostních mechanismů.

Reakce na útok a řešení následků

Ne vždy se však dá kybernetickému útoku zabránit. Je obecně známo, že nejslabším článkem je lidský faktor, který dříve nebo později selže. Ve chvíli, kdy je útok proveden, je nutné zareagovat co nejrychleji a tak, aby napáchal co nejméně škod.

Dojde-li například k vyřazení výrobní linky z provozu. Je její znovuuvedení v co nejkratším čase klíčovým úkolem, na který musí být společnost připravena, aniž by byl samotný útočník do této nápravy zapojen třeba tak, že by mu bylo vyplaceno výkupné.

Odstávka napadené výrobní linky znamená u špatně zabezpečené společnosti přerušení výroby i na několik týdnů, což má za následek nejen fatální finanční konsekvence, ale společnosti to může

značně poškodit i reputaci.

Vidíme do budoucnosti a umíme vás na ni připravit. Nabízím vám v tomto směru pomocnou ruku a partnerství s Accenture.