

Kyberbezpečnost je téma pro každého z nás

Teaser

IT technologie a online konektivita umožňují i vaší firmě rychleji růst, efektivněji hospodařit, rozvíjet byznys model a inovovat nabízené služby a produkty. Na druhou stranu se také stávají čím dál tím zranitelnější.

Jsem Michal Merta z Accenture a pokud bych měl pojmenovat jednu jedinou hrozbu, které by se měla každá společnost obávat a současně jí věnovat maximální pozornost, je to hrozba kybernetická.

Úvod

Žijeme v digitální době a připojení do internetu je samozřejmostí. Naše závislost na online světě a jeho možnostech nás vystavuje značnému riziku, které může zapříčinit dříve nebo později to, že uděláme chybu, které využijí útočníci.

Ze své více než patnáctileté zkušenosti v oblasti kyberbezpečnosti vím, že je útočníkovi vlastně jedno, jestli bude útok cílen konkrétně na vás a vaši firmu nebo půjde o náhodu.

Chyba vás bude stát v lepším případě "jen" hodně peněz. V tom horším bude narušeno naše vlastní soukromí nebo bezpečnost firmy, pro kterou pracujeme. Následkem může být poškození reputace, ztráta citlivých dat ale v krajních případech se lze obávat i o vlastní život.

Kyberútočník nepotřebuje důvod

Online závislost dělá skutečně z každé společnosti potenciální cíl, aniž by k tomu musel být nějaký důvod. A nejde jen o to, že vám nepozorný zaměstnanec smaže soubory.

Představa, že vaše firma je pro potenciální útočníky, chcete-li hackery nezajímavá, může být sice oprávněná, avšak podceňovat cyber security rozhodně není na místě. Ve valné většině kybernetických útoků je právě náhoda tím, co z vaší společnosti udělá cíl kybernetického útoku.

Zkušenost je taková, že se společnost náhodně připele do plošné kybernetické vlny útoku, jejíž následek může být krádež, ztráta nebo zablokování dat, poškození vaší technologie nebo její vyřazení z provozu, případně krádež know-how. A z této skutečně náhodně vzniklé situace se pak dlouhodobě vzpamatovává.

U nás v Accenture stojí celý náš byznys na kyberbezpečnosti. Jako poradenská společnost v oblasti digitálních technologií a Cloudu věnujeme vlastní kyber ochraně nejvyšší možnou prioritu – i proto můžeme naše klienty efektivně chránit. Ale před kým vlastně?

Hrozba má více podob

Řada z nás si hackery představí jen jako organizovanou skupinu expertů. Ale existují různé typy útočníků, před kterými je nutné se chránit a to bez ohledu na to, zdali mají, nebo nemají motiv.

Může se samozřejmě jednat o externí útočníky vystupující v podobě **organizovaných skupin**, které disponují obrovskými finančními zdroji, ještě větším výpočetním výkonem a těmi nejlepšími hackery.

Na opačné straně ale stojí jednotlivci z řad **vašich zhrzených zaměstnanců, nebo nespokojených klientů**. A není to pouze o cíleném útoku a detailní znalosti IT. Samo nebezpečí skýtá i neuvědomělé chování v kombinaci s nejrůznějšími digitálními viry a malwarem.

Útočit mohou i **jednotlivci**, které to prostě baví. Ať už si chtějí něco dokázat, někoho poškádlit, nebo jen přivydělat. Jejich motivace nebývá velká, ale přesto je výsledek jejich aktivity pro oběti útoků velkým problémem.

Za útokem mohou stát rovněž **státem řízené organizace**, které využívají kybernetických útoků k řešení svých mezinárodních zájmů a ovlivňování zahraniční politiky. Právě tyto útoky jsou v poslední době na vzestupu a státy je začínají využívat místo znatelně dražších vojenských operací. Cílem může být kromě ovlivňování politických zájmů rovněž ohrožení průmyslové nebo ekonomické sféry. Poškození reputace a dobrého jména, znemožnění, ohrožení národní bezpečnosti, nebo krádež citlivých dat a v neposlední řadě také peněz, to vše se děje a podotýkám ve velkém už dnes.

Víme proto, že ochrana kritické infrastruktury a samotná role státu v oblasti kyberbezpečnosti v budoucnu zdatelně poroste. Digitalizace, digitální identita, online fungování státní správy, to všechno bude třeba důsledně zabezpečit a ochránit tak občany – tedy každého z nás.

Věřím, že i vy vnímáte kyberbezpečnost jako důležité a neopomenutelné téma týkající se vašeho byznysu, které je nutné nebrat na lehkou váhu. Nabízím vám v tomto směru pomocnou ruku a partnerství s Accenture. A nejen já, ale celé naše Cyber Fusion Center, díky kterému se budete moci věnovat více svému byznysu a méně jeho ochraně, protože o ni se postaráme my v Accenture