■ Debata HN

Kyberútoky jsou na denním pořádku, firmy platí na výkupném miliony

Radek Kubeš
autori@hn.cz

Naše závislost na internetu a IT systémech stále roste a s tím i zranitelnost, kterou představují kybernetické útoky. Útoky, o kterých se dozvídáme z médií, jsou ale jen špičkou ledovce. „Skutečné množství úspěšných kyberútoků je nejméně o řád, možná i o několik řádů vyšší, než by bylo možné soudit podle veřejně dostupných informací. Ransomwarové útoky jsou prakticky na denním pořádku a firmy o nich nijak neinformují," řekl v únorové debatě Hospodářských novin o kybernetické bezpečnosti Josef Grill, zakladatel společnosti WEDOS Internet.

Jindřich Šavel, generální ředitel společnosti Novicom, techniku hackerů popisuje jako „střelbu z brokovnice" na nedostatečně zabezpečené firemní sítě a systémy. „Požadavek výkupného za zašifrovaná data je často až poslední fází útoku. Útočníci mohou být v síti své oběti třeba i několik let a až při svém odchodu si řeknou o peníze," dodává Šavel.

Do intenzity a závažnosti útoků se promítá i geopolitická situace, která mění „obchodní model" kybernetické kriminality. Útočníci jsou často za provedení útoků placeni hackerskými skupinami, někdy i podporovanými některými státy. „Převážnou většinu nedávných útoků, které zaznamenal český NÚKIB, má na svědomí hackerská skupina NoName057 hlásící se k Rusku, která nabízí platby dalším hackerům, útočícím pod jejich vlajkou," vysvětluje nárůst počtu kyberútoků Petr Kocmich, global cyber security delivery manager společnosti Soitron.

Propojení kybernetického světa s politikou jasně dokazuje i nárůst útoků po loňském napadení Ukrajiny Ruskem. Kybernetická válka se vede ze všech stran, potvrzuje Jaroslav Cihelka, jednatel společnosti ComSource: „Kromě útoků směřujících z Ruska například na naši veřejnou správu jsme zaznamenali i útoky na dezinformační weby a firmy, které se po vypuknutí války odmítly stáhnout z ruského trhu."

Bezpečnostní strategie místo výkupného

Zástupci českých firem na veřejnosti nemluví ani o výši zaplaceného výkupného po ransomwarových útocích. Jaroslav Cihelka ji odhaduje na statisíce až miliony korun v kryptoměnách. Takové firmy se ale mohou snadno stát obětí dalšího vydírání, protože vyděrači zjistí ochotu platit. Navíc neexistuje žádný postup, jak takové prostředky vykázat v účetnictví. I proto všichni účastníci diskuse doporučili zásadně výkupné neplatit.

Zranitelnost českých firem souvisí s podceňováním business continuity managementu neboli schopnosti organizace pokračovat v dodávkách produktů a služeb i po rušivém incidentu. Podle Jindřicha Šavela firmy často nevědí, co mají v případě útoku dělat a jak svůj provoz co nejrychleji obnovit. „Pokud by takové plány měly, tak jim sice obnova zabere třeba dva dny, ale nebudou donuceny platit výkupné."

Českým podnikům často chybí i úplný základ v podobě analýzy rizik, ze které pak vychází bezpečnostní strategie a střednědobý plán její realizace. „Přístup firem je v zásadě dvojí – některé podniky řeší každoročně dílčí bezpečnostní projekty, zatímco jiné mají strategii a koncepčně využívají svůj rozpočet na kybernetickou bezpečnost k její realizaci," popisuje Petr Kocmich. Často je ale problém investice do zabezpečení u managementu vůbec obhájit – alespoň dokud nedojde k nějakému incidentu. Josef Grill pak upozorňuje na skutečnost, že přestože jsou podniky na IT naprosto závislé, pro management mnohdy jde o „černou skříňku".

Mohou si firmy kyberbezpečnost dovolit?

Jakkoli nelze univerzálně stanovit výši nákladů na kybernetické zabezpečení firmy, nabízí se otázka, zdali mohou české podniky ochranu svých IT systémů a dat vůbec ufinancovat. Jaroslav Cihelka je přesvědčený, že přinejmenším středně velké firmy určitě ano. „Existuje řada systémů a služeb, včetně nabídky poskytovatelů cloudových služeb, které nabízejí alespoň základní úroveň zabezpečení. Ale stále zde zůstane rozpor mezi zajištěním provozu potřebného IT a kybernetickým zabezpečením – v rámci daného rozpočtu," vysvětluje Cihelka.

Jako klíčové se ukazuje vzdělávání zaměstnanců. A nejen jich – účastníci debaty se shodli, že výuka kyberbezpečnosti patří už na střední školy. Stát by tak mohl pomoci s řešením kritického nedostatku zaměstnanců v oblasti kybernetické bezpečnosti, který se dále prohlubuje.

Nové povinnosti pro tisíce firem

Žádná debata o kybernetické bezpečnosti se v současnosti nemůže vyhnout tématu evropské směrnice NIS2, která asi 6000 českých firem stanovuje nové povinnosti v této oblasti. „Dopad bude rozhodně větší než zavedení GDPR a už dnes se na nás obracejí firmy, které se na novou legislativu chtějí včas připravit. Zavedení NIS2 se rychle blíží," upozorňuje Jindřich Šavel ze společnosti Novicom.

Nová legislativa přinese odpovědnost konkrétních manažerů za kyberbezpečnost, stejně jako například nutnost pravidelných školení a bezpečnostních auditů. „Nové požadavky budou tlačit statutární zástupce firem k zavedení silných kyberbezpečnostních opatření. Otázkou je, jestli by podobný tlak neměl být také na firmy, kterých se NIS2 netýká," uvažuje Josef Grill, zakladatel společnosti WEDOS Internet.

Petr Kocmich ze společnosti Soitron ale upozorňuje, že bude problém získat bezpečnostní experty, kteří budou schopni nové požadavky ve firmách splnit. Proto dále poroste zájem o outsourcing kyberbezpečnostních služeb. „Zavedení NIS2 je krok správným směrem, protože směrnice podporuje i spolupráci a sdílení informací v oblasti kybernetických rizik," dodává Jaroslav Cihelka ze společnosti ComSource.

Petr Kocmich
global cyber security delivery manager, Soitron

Jaroslav Cihelka
jednatel, ComSource

Josef Grill
zakladatel, WEDOS Internet

Jindřich Šavel
generální ředitel, Novicom

Foto: HN – Matej Slávik

Ransomwarové útoky jsou prakticky na denním pořádku a firmy o nich nijak neinformují.
Josef Grill, WEDOS Internet

Útočníci mohou být v síti své oběti třeba i několik let a až při svém odchodu si řeknou o peníze.
Jindřich Šavel, Novicom

Směrnice NIS2 podporuje i spolupráci a sdílení informací v oblasti kybernetických rizik
Petr Kocmich, Soitron

Kromě útoků z Ruska jsme zaznamenali i útoky na dezinformační weby a firmy, které se odmítly stáhnout z ruského trhu.
Jaroslav Cihelka, ComSource