Spoločnosť verí falošnému pocitu bezpečia, upozorňuje popredný slovenský IT vývojár

REDAKCIA CYBERSEC | 25.11.2015 SLOVENSKÁ REPUBLIKA

Kybernetická ochrana už dávno nepredstavuje výsostnú doménu vládnych agentúr. Práve naopak, so zvyšujúcou sa pravdepodobnosťou kybernetických útokov s čoraz vážnejšími následkami je nevyhnutné podporovať obojstranne výhodné partnerstvo verejného a súkromného sektora. O tom, ako vníma kybernetickú ochranu a partnerstvo štátnych a neštátnych aktérov na Slovensku a aké odpovede na kybernetické hrozby ponúka spoločnosť, ktorú reprezentuje, sa portál CyberSec.sk porozprával s Petrom Dostálom, generálnym riaditeľom spoločnosti Aliter Technologies, a.s., poprednou vývojárskou a poradenskou spoločnosťou v oblasti informačných a komunikačných technológií, ktorej sa úspešne darí presadiť sa aj v tvrdej zahraničnej konkurencii.

Začnime trochu všeobecne. Kybernetické ohrozenia sú jednými z tých, ktorým sa v posledných rokoch celosvetovo venuje obrovská pozornosť. No na Slovensku akoby sa tieto hrozby stále podceňovali a verejnosť si neuvedomuje ich možné negatívne dôsledky. Ako hodnotíte celkové povedomie a úroveň opatrení voči týmto problémom?

Každá krajina má obmedzené prostriedky a definuje si svoje priority. Denne z médií počúvame o nedostatku peňazí pre zdravotníctvo alebo školstvo. Budovanie kybernetickej bezpečnosti si vyžaduje investície, ktoré na prvý pohľad neprinášajú žiadne služby občanom a ani neprispievajú k zjednodušeniu a automatizácii procesov a činností. Nakoľko na Slovensku nie sú verejne známe žiadne väčšie dôsledky prípadných kybernetických útokov, nestala sa kybernetická bezpečnosť prioritou pre spoločnosť ani štátnu správu. Situáciu možno prirovnať k stavu investovania do ozbrojených síl. Spoločnosť pod vplyvom falošného pocitu bezpečia dlhé roky nepovažovala za potrebné investovať do modernizácie ozbrojených síl. Bezpečnostné incidenty z posledných rokov nás presvedčili, aká môže byť bezpečnosť krehká, a aké potrebné je byť pripravený. Je dôležité, aby si vlastníci a používatelia informačných systémov uvedomili vplyv nedostupnosti týchto systémov, respektíve ich zneužitie. Takmer všetky časti našej spoločnosti sú priamo alebo nepriamo závislé od informačných systémov.

Investuje slovenská spoločnosť, vrátane štátnej správy, do oblasti kybernetickej bezpečnosti dosť?

Dostatočná investícia do kybernetickej bezpečnosti je relatívny pojem. Ani hľadanie najlepšieho pomeru cena/výkon nemusí viesť k najlepšiemu riešeniu. Vláda v tomto roku prijala koncepciu kybernetickej bezpečnosti na Slovensku a zadefinovala súvisiace kompetencie a zodpovednosti orgánov štátnej správy. Príslušné orgány by mali následne spracovať rizikové a dopadové analýzy a navrhnúť potrebnú legislatívu, politiky, procesy a technológie na zvýšenie kybernetickej bezpečnosti na požadovanú úroveň. Treba povedať, že v súčasnosti prebieha už niekoľko iniciatív na rezortných úrovniach.

Vaša spoločnosť je tiež členom Združenia bezpečnostného a obranného priemyslu. Ako by mal štát pomáhať rozvoju tohto segmentu? Čo by mohlo pomôcť slovenským firmám k úspechu pri medzinárodných projektoch?

Skúsim zopár konkrétnych príkladov, kde štát môže pomôcť a vo viacerých prípadoch aj pomáha. Po prvé, pre úspech slovenských bezpečnostných a obranných technológií v zahraničí je dôležité, že sú zavedené do výzbroje Ozbrojených síl SR. OS SR môže pomôcť konzultáciami, testovaním, ukážkami a referenciami. Po druhé, štát participuje na medzinárodných projektoch a má možnosť ich prostredníctvom presadzovať záujmy slovenského bezpečnostného a obranného priemyslu. Je dôležité, aby štátna správa mala prehľad o produktovom a službovom portfóliu slovenských subjektov, vrátane tých komerčných. Musíme sa zbaviť dojmu, že pomoc štátu komerčným subjektom je niečo negatívne. Veď nakoniec tie subjekty tu zamestnávajú ľudí, platia odvody a dane, sú súčasťou našej spoločnosti. Po tretie, štátna správa má svojich zástupcov v medzinárodných organizáciách a môže prostredníctvom nich presadzovať záujmy slovenského bezpečnostného a obranného priemyslu rovnako ako to robia zástupcovia iných krajín. Príklad si môžeme vziať aj z menších krajín, ako je napríklad Dánsko. Aj u nás si pamätám, že v minulosti zavítali aj špecialisti na obstarávanie v rámci NATO. To je správna cesta. Na druhej strane si komerčné subjekty musia uvedomiť, že ak nevedia ponúknuť komerčne zaujímavé produkty a služby, tak im ani štát nedokáže efektívne pomôcť ich predať v zahraničí. V niektorých regiónoch je pomoc štátu limitovaná a komerčné subjekty si musia hľadať aj alternatívne cesty. Naša spoločnosť napríklad založila dcérsku spoločnosť v Kanade, aby sme pomocou nej urýchlili náš vstup na severoamerický trh.

V zahraničí sa Vám celkom darí. Tento rok ste boli jedinou slovenskou spoločnosťou, ktorá na medzinárodnom veľtrhu obrannej a bezpečnostnej techniky v Brne získala jedno z hlavných ocenení Zlatý IDET 2015 za hlasovú komunikačnú bránu. Priblížte nám toto zariadenie.
Tento svojimi rozmermi malý a nenápadný produkt umožňuje integráciu bojových a komerčných rádiových sietí s analógovými, digitálnymi, mobilnými a VoIP sieťami. Produkt je kompletne navrhnutý a vyrobený na Slovensku. Spĺňa vojenské štandardy USA, získal viacero ocenení a okrem slovenských ozbrojených síl ho využívajú aj ozbrojené sily iných krajín. Je tiež súčasťou projektov nadnárodných spoločností ako sú napríklad Airbus Defence and Space a Northrop Grumman.

Jednou z oblastí, na ktorú sa zameriavate, je informačná a technologická bezpečnosť dátových centier. Veľa sa hovorí o bezpečnosti cloudov. Sú ohrozené?

Ďalším evolučným krokom pri vývoji dátových centier je cloud computing. Na jednej strane cloud priniesol so sebou efektívnejšie využívanie prostriedkov a zaviedol štandardy a automatizáciu do prevádzky informačných systémov, ale na druhej strane so sebou prináša nové bezpečnostné riziká

spojené s využívaním zdieľaných zdrojov akými sú servery, prepínače, smerovače, ale aj nástroje bezpečnosti ako sú firewally, IDS, IPS systémy a podobne. Odhliadnuc od toho či sa jedná o verejný, privátny alebo hybridný cloud, všetky využívajú zdieľané prostriedky a ich virtualizáciu. Preto je nesmierne dôležité zabezpečiť izoláciu a kontrolovanú komunikáciu medzi jednotlivými systémami využívajúcimi prostredie cloudu. Je nesmierne dôležité dôsledne navrhnúť logickú a fyzickú topológiu siete a doplniť ju o najmodernejšie bezpečnostné technológie. Rovnako dôležité je mať prehľad o stave prostredí a bezpečnostnej situácii prostredníctvom monitorovacích nástrojov. Následne konzistenciu cloudu a dodržiavanie bezpečnostných a prevádzkových politík zabezpečiť prostredníctvom orchestračných a automatizačných nástrojov. A toto je práve oblasť, vývoju ktorej sa my intenzívne venujeme už dlhšie obdobie.

Na aké typy bezpečnostných hrozieb sa najviac zameriavate?

Asi najviac sa venujeme bezpečnostným hrozbám vedeným voči IKT infraštruktúre: to znamená útoky voči sieťam, dátovým centrám, operačným systémom a podobne. Rovnako venujeme zvýšenú pozornosť bezpečnostným hrozbám vedeným voči informačným systémom prostredníctvom nedôsledne zabezpečenej IKT infraštruktúre.

Navrhujete bezpečnostné systémy pre iných, ale ako ste na tom vy? Boli ste niekedy terčom kybernetického incidentu?

Viem, že sa hovorí, že obuvníkove deti chodia bosé, ale v tomto prípade my bezpečnosť vlastných systémov a dát neberieme na ľahkú váhu. Požívame rovnaké technológie a postupy, aké odporúčame aj našim zákazníkom a možno aj preto môžem nateraz konštatovať, že k žiadnemu vážnejšiemu kybernetickému incidentu u nás nedošlo.