Jeffrey Bardin

Je hlavním zpravodajským důstojníkem pro Treadstone 71. Jeff pracoval ve vedoucích pozicích organizací, jako jsou General Electric, Lockheed Martin a Marriott International. Sloužil v USAF jako kryptologický lingvista a v USANG na pozici Armored Scout Platoon Leader.

Nemělo by být dovoleno prodávat počítačové produkty, které nedosahují určité úrovně bezpečnosti

Ve své přednášce na konferenci IS2 jste představil překvapivou koncepci, podle níž kybernetická bezpečnost nemůže stát jen na obranných opatřeních, ale je zapotřebí nebát se útočit. Můžete to vysvětlit blíže?

Ta myšlenka je nová ve virtuálním prostředí, ale z perspektivy fyzické obrany je stará a osvědčená. Ať už bráníte cokoli, nedokážete to, pokud spolu s obrannými opatřeními nepodnikáte protiútoky. Jinak nedokážete nepřátelské aktivity zastavit a útočník dříve či později uspěje. To platí, ať už hájíte pevnost, nebo hrajete míčovou hru… Že to platí i v kybernetické bezpečnosti, je nejlépe patrné u organizací, které utratily obrovské prostředky, vyvíjejí obrovskou snahu a stále znovu a znovu přicházejí o data. Bezpečnost založená na obraně zkrátka nefunguje.

Když bráníte pobřeží, stanovíte určitou zónu a napadáte útočníka ještě předtím, než přistane. Když ale bráníme své počítačové sítě, čekáme, až se útočník dostane dovnitř, teprve potom podnikáme akci. Fakticky se pokoušíme zmírnit následky útoku, který již do určité míry uspěl, nesnažíme se mu zamezit. Jsme zvyklí, že nemůžeme na někoho jen tak zaútočit. Samozřejmě, v komerčním prostředí jsou určité hranice toho, co je přijatelné. Ale většinu útoků provádějí hackerské skupiny a jiné kriminální organizace. A tady je možné určité kroky podnikat. Zaprvé je zapotřebí provádět protiúder včas a ne až poté, co se útočník dostal do vaší sítě. Zadruhé je možné podnikat určitá odvetná opatření.

„Ukazuje se, že tam, kde mluvíme o slabé IT bezpečnosti, se ve skutečnosti jedná o špatně vybudované IT. To nemohou řešit bezpečnostní specialisté.“

Jak vidíte vztah mezi správou informačních systémů a počítačovou bezpečností?

Bezpečnost je až druhým krokem. V první řadě záleží na tom, jak jsou informační systémy budovány. Zda je jejich ochrana dost robustní a zda je jejich architektura nečiní zbytečně zranitelnými. Existují třeba systémy, které jsou 24 hodin denně připojeny k internetu, i když to fakticky není zapotřebí. Potřebují jen občasný servisní zásah nebo aktualizaci. Takových zbytečně vytvářených slabých míst existuje celá řada. Ukazuje se, že

tam, kde mluvíme o slabé IT bezpečnosti, se ve skutečnosti jedná o špatně vybudované IT. To nemohou řešit bezpečnostní specialisté. V takových případech je jediná rada: nejprve si udělejte pořádek v tom, jak jsou postaveny vaše systémy. Protože pokud budete provozovat chybně koncipované systémy a budete se je snažit „doplnit“ o bezpečnost, utratíte obrovské prostředky, a přesto nebudete s výsledkem spokojeni.

Ve Spojených státech zavádíme nové věci příliš rychle a staráme se jen o komerční stránku. Každý chce mít výrobek na trhu dříve než ostatní, a to i za cenu, že není dobře postaven. Typicky se říká, to opravíme za pochodu. Takže se navrhují zařízení a systémy, kde se architekti bezpečností příliš nezdržují. Po čase se ukáže, že ta zařízení jsou zranitelná, a dodělává se k nim bezpečnost. Ale to už je příliš pozdě. Nikdy nedosáhneme stejné úrovně bezpečnosti, jako kdybychom ji měli na zřeteli od začátku. A postupuje se tak dokonce u zdravotnické techniky! Je to stejné, jako kdybychom uvedli na trh auto bez brzd a až po pár nehodách je začali dodělávat. Zkuste si představit, na kolik by vyšlo dodatečné přidělání brzd k již hotovému modelu. Z pohledu finančních výsledků za momentální finanční období by to možná vyšlo výhodněji. Ale samozřejmě by to byl nesmysl. Pokud věc není dost bezpečná, je nepoužitelná. V Americe říkáme, že auto má brzdy především proto, aby mohlo jezdit rychle. S počítači je to stejné.

Jak to ale řešit? Výrobci budou vždy upřednostňovat finanční výsledky a zákazník není schopen posoudit, jestli je systém dost bezpečný.

Tady by měl nastoupit regulátor. Když konstruktéři navrhují nový model, od začátku vědí, že bude mít brzdy, bezpečnostní pásy, airbagy a další zařízení. Protože vědí, že jinak by se takový model nesměl prodávat. Na druhou stranu však žádný regulátor neříká, jak mají být brzdy, světla nebo bezpečnostní pásy zkonstruovány. Říká jen, jaké mají mít funkce a při jakých testech mají obstát. Takhle funguje správná regulace. Podle mě bychom se měli na počítačová zařízení dívat stejně. Nemělo by být dovoleno prodávat produkty, které nedosahují určité úrovně bezpečnosti. Měly by být definovány minimální požadavky z hlediska administrace, provozu, přístupů, fyzické bezpečnosti atd. Máme regulace na všechno možné a nemožné, ale kybernetickou bezpečnost trestuhodně podceňujeme.

Nehraje v tom roli také to, že uživatelé nejsou ochotni platit za zvýšenou bezpečnost?

To je další část problému. Většina uživatelů neví, o co jde. Nedokážou si představit, co všechno se může stát. I kdyby si to dokázali představit, nevěděli by, jak produkt posoudit. To se ostatně netýká jen nákupu zařízení. Většina uživatelů neví nic o bezpečném používání počítače a bezpečném chování na internetu. Měli bychom je učit, co mají požadovat od výrobců, a především jak se chovat, aby chránili sebe i ostatní. Pro spoustu uživatelů to je vzdálená technická záležitost, musíme jim to opakovat znovu a znovu, dokud nezačnou měnit své chování. Dokud se nestane úplně samozřejmým, že některé věci se nedělají.

Když jdete do lesa a vidíte tam hada, nesnažíte se ho pohladit. Nikdo se o to nesnaží. Ale když přijde e-mail od neznámého odesilatele, spousta lidí klikne na odkaz. Na tom je vidět, jak hrozně chybí vzdělání. Byl bych pro to, aby každý musel povinně projít základním kurzem informační bezpečnosti. V řadě států USA je tomu tak, že když si kupujete střelnou zbraň, musíte ukázat potvrzení o absolvování základního kurzu bezpečného zacházení se zbraněmi. S počítačem by to mělo být podobně.

Tedy něco jako řidičský průkaz na počítač?

Přesně tak. To není žádné omezení, prostě dostanete potřebné školení. Vedle řidičského průkazu byste měl průkaz pro brouzdání po internetu. Lidé se dnes mnohdy chovají bláznivě, nepoškozují tím jen sebe, ale i své blízké. Zaměstnavatelé by tomu měli věnovat pozornost při přijímání nových zaměstnanců. Jestliže někdo publikuje na sociálních sítích informace o svých blízkých nebo tam třeba věší choulostivé fotografie, můžete předpokládat, že se bude podobně chovat i jako zaměstnanec.

Lidé ale nebudou nadšení z toho, že jim vláda stanoví další a další pravidla. A už vůbec z toho nebudou nadšení lidé od počítačů.

Přesto by k tomu mělo dojít. Vím, že se lidem těžko říká, že mají být zavedeny další regulace. Ale v rámci bezpečnosti regulace opravdu fungují. Dokázali jsme přimět lidi, aby používali bezpečnostní pásy, a nikdo si dnes nestěžuje. Spousta jiných regulací dobře funguje ve zdravotnictví, energetice a dalších oborech. Uvědomuji si, že musí být určitá rovnováha mezi tím, čeho chceme dosáhnout, a tím, co můžeme od občanů požadovat a jaké informace o nich shromažďovat. Ale v tomto případě jsou rizika natolik velká, aby regulace ospravedlnila.

Jenže ono to taky může skončit tak, že úřady vytvoří nějaký naprosto nepoužitelný dokument, budou se vytvářet zbytečné výkazy a třeba falšovat záznamy o účasti na školeních.

Zbytečné výkazy a kontrolní seznamy máme teď. Nějaké regulace existují, ať už je prosazují regulátoři různých odvětví, nebo odvětvová sdružení, takže jde fakticky o seberegulace. Řada organizací k nim přistupuje zcela formálně. Mohou si to dovolit, protože vzhledem k jejich byznysu je to vedlejší. Žádný šéf informační bezpečnosti se neodváží přijít a říct: „Musíme udělat to a to, i když nám to zpomalí vývoj produktů a sníží zisk.“ Kdyby to bylo tak, že bez dosažení stanovené úrovně bezpečnosti nebude možné pokračovat v činnosti, stejně jako výrobce aut nesmí prodat vozidlo bez brzd, věnovali by tomu mnohem větší pozornost.

Možná se ochota akceptovat v této oblasti regulace zvýší s internetem věcí. Přece jenom může mít napadení automobilu nebo domu dramaticky vážnější následky než vykradení bankovního účtu.

Ano, jedu po dálnici a někdo převezme řízení mého vozu. Může zrychlit, zpomalit, vypnout motor nebo třeba odpojit brzdy, protože je to řízené počítačem. To je bláznivé. Nebo někdo může na dálku ovlivnit třeba nějaké zdravotní zařízení, které mám na těle, poslat nesmyslné pokyny a chybné informace mému lékaři. Ale obávám se, že ani když půjde o život, se firmy nebudou držet zásady „bezpečnost především“, ale „zisk především“, a bezpečnostní funkce se budou řešit dodatečně. Nyní se ve Spojených státech diskutuje o možnosti hacknout dopravní letadlo, protože se zjistilo, že byla do provozu uvedena letadla, kde není řídicí systém oddělen od zábavního, ke kterému mohou přistupovat všichni cestující bez omezení!

Tím se vracíme zpět k podnikové bezpečnosti. Když říkáte, že součástí kybernetické bezpečnosti by měly být také protiútoky, jak je to možné aplikovat v podniku?

Můžete např. shromažďovat informace o svých konkurentech nebo jiných

„Je zajímavé, že CISO potřebuje spoustu speciálních školení a certifikací, jako jsou CISSP a CISM, zatímco pro IT manažera neexistuje žádná povinná úroveň znalostí.“

organizacích, které by mohly potenciálně stát za vaším napadením. Neporušujete žádný zákon tím, že víte, jací lidé tam pracují, kam chodili do školy, jak často jsou na internetu, jaký obsah publikují na sociálních sítích, jaké systémy používají atd. Nemusíte kvůli tomu ani pronikat do jejich systémů a zařízení – existují chaty, blogy, Twitter, Facebook, Pinterest, Instagram, Youtube. Můžete to provádět naprosto anonymně, optimálně z počítačů, které nejsou připojeny k vaší firemní síti.

Jakmile máte dostatek informací, můžete s nimi pracovat. Někdy vám pomohou připravit se na útok, jindy je můžete poskytnout třetí straně a požádat ji o určitou službu. Vlády to dělají dlouhodobě. Jsou skupiny, které na internetu bojují za nás, a jsou skupiny bojující třeba za Rusy. Vlády je podporují finančně a jinak, ale nepřebírají za ně odpovědnost. K takovým možnostem je ale potřeba přistupovat se značnou zdrženlivostí, kdyby jiné cesty selhaly.

A co shromažďování informací o zaměstnancích? Říká se, že vlastní lidé jsou nejčastější příčinou prolomení obrany, a to i na poli kybernetické bezpečnosti.

Pochopitelně. Než začnete shromažďovat informace o někom jiném, měl byste toho vědět dost o sobě. Tedy podívat se na sebe a vlastní slabá místa. Vědět, kteří zaměstnanci jsou na kterých sociálních sítích, co tam dělají, co říkají, do kterých skupin jsou zapojeni. Někdo možná namítne, že je to neetické. Ale nezapomínejme, že to jsou informace, které sami zaměstnanci sdělují. Rozhodně je z chování na sociálních sítích možné usuzovat, kteří zaměstnanci by případně byli ochotni prozradit důvěrnou informaci nebo třeba přístupové údaje. Můžete se pak speciálně zaměřit na jejich školení a motivaci, případně můžete nasadit softwarové nástroje, které jim zabrání dělat určité věci. Je podstatné, abyste jim pomohli změnit chování nejen na pracovišti a během pracovní doby, ale i mimo práci. Samozřejmě můžete narazit na otázky důvěrnosti a na to, nakolik je možné zasahovat do osobního života zaměstnance. Ale snažíte se přece zastavit riskantní chování, které ohrožuje firmu.

Ostatně, jsou případy, kdy někdo způsobí autonehodu pod vlivem alkoholu nebo se dopustí jiného zločinu a je za to propuštěn ze zaměstnání, i když k tomu došlo ve volném čase. Proč bychom neměli podobně přistupovat k chování na internetu? Ale souhlasím, že to není snadná záležitost. Je zapotřebí pečlivě zvažovat, kam je ještě možné zajít a kam už ne.

Jaká by měla být optimální pozice CISO v podniku?

V mnoha firmách jsme svědky střetu zájmů mezi CISO a CIO. CIO je odpovědný za celou informatiku, bezpečnost je pro něj jen jednou z oblastí, a to nikoli oblastí prioritní. Zase se dostáváme k tomu, o čem jsme už hovořili. IT není vybudováno tak, aby bylo dostatečně bezpečné, a šéfům informatiky to vlastně až tak nevadí. Přitom žádný z nich by neodešel ze svého domu či bytu, aniž by zamknul dveře a zavřel okna. Neodjel by na dovolenou bez zapnutí alarmu. Prostě udělá všechno, co je v jeho silách. A ten stejný člověk prokazuje až neuvěřitelnou lehkomyslnost, jde-li o bezpečnost informací ve svém podniku. Potřebujeme IT manažery, kteří budou o data pečovat se stejnou důkladností, s jakou brání své domy proti vykradení.

Když IT manažer takový přístup nemá, vznikají konflikty. Buď k nim dochází tak, že manažer odpovědný za informační bezpečnost říká: „Architektura je chybná. Systémy by měly být koncipovány jinak. Za současného stavu není možné dosáhnout rozumné úrovně bezpečnosti.“ Nebo dochází k tomu, že to bezpečnostní manažer neříká, protože je podřízený IT manažerovi a bojí se, že přijde o místo. Sám jsem byl jednou vyhozen z práce za to, že jsem napsal do reportu, že naše IT prostředí nevyhovuje standardům požadovaným regulátorem, a šéfovi IT se to nelíbilo. Vrátil jsem se z dovolené a zjistil jsem, že report byl zamítnut a já už ve firmě nepracuju. Prostě chtěl za každou cenu zabránit rozšíření té informace do zbytku společnosti.

> „Je zapotřebí provádět protiúder včas a ne až poté, co se útočník dostal do vaší sítě. Je také možné podnikat určitá odvetná opatření. “

Myslím, že každý šéf IT by měl nejdřív pracovat alespoň tři roky na pozici CISO. Je zajímavé, že CISO potřebuje spoustu speciálních školení a certifikací, jako jsou CISSP, CISM. Zatímco pro IT manažera neexistuje žádná povinná úroveň znalostí. IT manažerem se může stát každý. Dokud se to nezmění, jsem pro, aby pozice CISO byla nezávislá na IT. Je to příliš důležité, než aby bezpečnost byla jedním z útvarů mezi infrastrukturou, databázemi a zákaznickou podporou.

Ptal se Petr Hampl.