Je nutno čelit nepříjemné pravdě a tou je, že bezpečnost dat a informačních aktiv musí vycházet od vedení organizace

řekl CzechIndustry Tomáš Hlavsa, Business Development Manager divize Big Data and Security, Atos IT Solutions and Services

Mezi nejvážnější hrozby, jimž čelí lidstvo, patří ty, které se odehrávají v kyberprostoru? Co vše tento pojem zahrnuje a která jsou hlavní ohrožení?

Definici kyberprostoru bych přenechal filosofům, nicméně z našeho pohledu kyberprostor zahrnuje všechna zařízení, komunikační a úložné prostředky, ale také osoby, které přicházejí do kontaktu s našimi daty a informacemi v nich obsaženými. V běžném životě tedy veškeré mobilní telefony, počítače, počítačové aplikace, digitální média a cloudová prostředí. Výčet není úplný, ale již jen z uvedeného je patrné, že se jedná o velkou část předmětů, které v každodenním životě používáme.

Část hrozeb jsme se naučili již rutinně řešit. Ztráta mobilního telefonu je dnes spíše nepříjemností, než vážným problémem. Obnova ztracených či poškozených dat je rovněž rutinní operací.

Co je však z našeho pohledu závažné, jsou nenápadné útoky, které jsou dlouhodobě nedetekovány. Nedetekované průniky do našich osobních počítačů jsou jistě osobně velmi nepříjemné, ale nedetekovaný průnik do průmyslových, energetických, či zdravotnických infrastruktur má potenciál ohrozit množství lidských životů a způsobit finanční a materiální ztráty značného rozsahu. V té souvislosti je patrný nárůst i vysoké organizovanosti a nárůst záběru kyberkriminality. Přičemž s nezadržitelným nárůstem propojování elektrických spotřebičů (ledničky, televize, domácí spotřebiče) do větších celků se exponenciálně zvětšuje i prostor pro nástup budoucích kyber útoků.

Kyberkriminalita je společenským problémem, nedávno se v jednom článku uvádělo, že kybernetickým útokům již nelze zcela zabránit. Tomu rozumím, nicméně podle mého se dají eliminovat jejich dopady?

Stav ohledně prevence versus eliminace dopadů v souvislosti s kyberkriminalitou má aktuální příměr v situaci týkající se uprchlíků z Afriky, či Blízkého východu. Celospolečenská diskuze, politická prohlášení a mediální obraz se téměř výhradně zaměřují na dopady této situace, vyjmenovává a rozebírá rizika, která v souvislosti s ní vyvstávají. Minimum ohlasů se zabývá její příčinou a téměř nikdo není schopen navrhnout reálné řešení příčin této „uprchlické situace".

S kyberkriminalitou je to podobné. Společnosti, vlády, úřady i jednotlivci mají povědomí o tom, co je třeba dělat v případě kyberzločinu/kyberútoku. Ať již se bavíme o virech, malware, DDOS útocích, phishingu, či fyzických ztrátách dat. Virů a malware se zbavit umíme, DDOS útoky jaktakž zvládáme, následky phishingu, je-li zjištěn, pokrýt také zvládneme. Přijdeme-li o data, obnovíme je ze záloh atp.

V čem však tápeme je prevence, vzdělávání a dlouhodobý systematický přístup. Technologicky prevence není obtížná. IPS, IDS systémy, DLP (Data Leakage Prevention) řešení, SIEM (Security Incident Event Management) sestavy, to vše jsou řešení dlouho známá a velmi účinná. Pracují však s těmito systémy spolehliví a proškolení lidé? Jsou technologická opatření v souladu s procesy, nařízeními a realitou naší firmy, našeho úřadu? Je bezpečnostní projekt, který nyní realizujeme jednorázovým opatřením, nebo budeme bezpečnost „budovat" dlouhodobě?

Zde je nutno čelit nepříjemné pravdě a tou je, že bezpečnost dat a informačních aktiv musí vycházet od vedení organizace. Ať je to management firmy, vedení úřadu, ministerstva či jiné instituce, je nutné, aby bezpečnost informací byla vyžadována vedením organizace. Bez jeho podpory je zavádění bezpečnosti (personální, procesní, fyzické, technologické) odsouzeno nutně k neúspěchu.

Prakticky od počátku IT technologií můžeme sledovat dva „protichůdné" směry. Na jedné straně jsou ti, kteří vytvářejí bezpečnostní systémy a na druhé ti, jež se je snaží zneužít. ATOS se zabývá počítačovou bezpečností již řadu let. Můžete nám přiblížit její vývoj ve společnosti?

To je téma na samostatný článek, navíc by vyžadoval pečlivou rešeršní přípravu. Napsat jej „jen tak, od stolu" by bylo nezodpovědné a neférové...

Rukopis ATOSu nese řada publikací věnovaných kybernetické bezpečnosti, jež jsou ke stažení na vašich www stránkách. Které z nich by si měli přečíst ti, kteří se zajímají o danou problematiku a proč?

Krátký, ale poměrně výstižný je článek „Privacy and Personal Data Protection" o ochraně osobních dat, případně článek „Industry 4.0" o sbližování kyber a fyzického světa.

Co vše dnes nabízíte firmám a společnostem z oblasti kybernetické bezpečnosti?

Namísto vyjmenovávání jednotlivých řešení, produktů nebo služeb uvedu jediné: Ucelený pohled. Nevnucujeme firmám, úřadům a jednotlivcům naše řešení. Naslouchámě, co v oblasti ochrany dat a informací potřebují. Nemáme pocit, že bychom potřebám našich zákazníků rozuměli lépe než oni. Ale ano, pakliže porozumíme potřebám zákazníka v oblasti kybernetické bezpečnosti, jsme díky velikosti naší firmy, mezinárodnímu přesahu a interdisciplinárním záběru schopní nalézt, navrhnout a dodat řešení, které zákazníkovu potřebu pokryje.

Na prvním místě je však vždy, vždy a vždy systematický přístup. Tedy neohýbat zákazníkovy procesy a prostředí do souladu s naším technologickým řešením, ale naopak ohnout naše řešení tak, aby zapadlo do procesů a prostředí zákazníka. Takový přístup si žádá určitou standardizaci a zde se krom legislativních omezení řídíme i mezinárodními standardy (v oblasti bezpečnosti např. rodina norem IS 27000) a v neposlední řadě i vnitřními politikami a předpisy konkrétního zákazníka.

Mohou firmy získat náskok před kyberzločinci a za jakých podmínek?

Toto je často diskutované téma na nejrůznějších konferencích, odborných fórech apod. Odpověď je šalamounská, ano i ne. Záleží, z jaké strany se na problém bezpečnosti díváme.

Ne, kyberzločinci budou mít z principu vždy logicky navrch nad jakýmkoliv zabezpečením. Ať již fyzickým (zámky, mříže, závory, trezory), technologickým (firewally, antiviry, IPS, SIEMy…), procesním (předpisy, omezení), legislativním (zákony, vyhlášky) či personálním (selhání jednotlivce).

Nikdy v historii lidstva nebyl vyvinut systém, či opatření, které by nebylo možno překonat. Vždy se najdou lidé, kteří dříve či později naleznou slabinu a zabezpečení překonají. Bylo tomu tak vždy a bude tomu tak nadále.

Na druhou stranu, ANO, lze získat náskok před kyberzločinci. Koneckonců jsou to také jen lidé. Otázka však stojí, jak moc úsilí chceme do ochrany našich hodnot investovat. Víme, která data jsou pro nás cenná a která ne? Jsme si vědomi všech rizik, která mohou naše aktiva ohrozit? A pokud ano, jsme schopni (personálně, procesně, technologicky) a ochotni (finančně) tato rizika eliminovat?

Znovu se vrátím k paralele s ochranou platidel. Bankovky a mince vnímáme a máme zažity jako hodnoty, které je záhodno chránit. Ochrana platidel se vyvíjela stovky let a za tu dobu se vyvinula do té míry, že padělání bankovek je v zásadě ojedinělým a přísně postihovaným jevem. V této oblasti života si dovolím říci, že vlády mají před zločinci náskok. Pokud vlády, společnosti a jednotlivci vyvinou podobné úsilí pro ochranu a bezpečnost informací, potom lze hovořit o minimálně náskoku před kyberzločinci.

Čelit bezpečnostním hrozbám v kyberprostoru vyžaduje předvídat trendy stále více digitalizované světové ekonomiky. Svědčí o tom dokument ATOSu nazvaný Journey 2018. Your business technologists. Powering progress the 3rd digital revolution agility and fragility. Takže, co nás čeká z pohledu technického vývoje v oboru IT v nejbližších letech?

Toto je na samostatné zamyšlení, nejsem technologický vizionář...

Drží podle Vás Česká republika z hlediska kybernetické bezpečnosti krok s vyspělým světem nebo máme co dohánět?

Čeká republika je v rámci Evropské unie jednou z prvních zemí, která přijala a zavádí legislativu v oblasti kybernetické bezpečnosti. Z tohoto pohledu se tedy řadíme k vyspělým zemím. V oblasti soukromých firem, domácností, akademické sféry je obecné povědomí o bezpečnostních hrozbách na obecně dobré úrovni. Druhou stranou této mince ovšem je reálná aplikace zákonných norem v oblasti státní správy. Zde situaci komplikují zejména nízká platová ohodnocení odborníků na bezpečnost a rovněž jistá procesní strnulost. Kde z našeho pohledu Česká republika, resp. oblast státní má co dohánět, je schopnost získávat, vzdělávat a především udržet bezpečnostní odborníky. Dokud orgány státní správy, ministerstva, úřady a státem řízené instituce nebudou schopny získat či vychovat kvalitní odborníky, tyto dlouhodobě vzdělávat a motivovat pro setrvání ve státních službách, bude se rozdíl v oblasti kybernetické bezpečnosti mezi soukromým a státním sektorem i nadále zvětšovat.

Čtvrtá průmyslová revoluce již není jen vizí, ale stává se skutečností. Významnou roli v ní budou hrát data a práce s nimi včetně jejich bezpečnosti. Jste v ATOSu připraveni na tuto výzvu?

Data, jejich bezpečné uchovávání, přenos a zpracování je téma, kterým se zabývají desítky firem. Pravidelně se v médiích, na konferencích i odborných časopisech prezentují odhady o budoucím nárůstu objemu dat a neustále rostoucí potřebě data ukládat. Výrobci síťových technologií vyzdvihují čísla o přenesených datech. Výrobci bezpečnostních technologií zveřejňují neuvěřitelné počty nových hrozeb, virů, malwarů atp. Skutečně však všechna ta data, gigabitové linky a nejnovější anti malware skenery souvisí s reálnou výrobou? Tedy s tím, co společnosti, úřady, domácnosti ke své činnosti a každodenní práci potřebují. Kolik dat reálně potřebujeme. A je doopravdy potřebné všechna naše data chránit? Jsme přesvědčeni, že na trhu vzniká určitá řekněme bezpečnostní bublina, uměle přiživovaná společnostmi, které ve snaze udržet zisk, prodeje generují a přiživují poptávku po technologických řešeních.

ATOS je přesvědčen, že skutečná potřeba bezpečnosti dat a informací spočívá v systematické a dlouhodobé práci s lidmi, kteří data vytvářejí, s informacemi v nich pracují a používají je ku prospěchu svému, či svého zaměstnavatele. Na základě této premisy ATOS staví svou strategii v oblasti bezpečnosti informací. Konkrétně jde o identifikace reálné potřeby ochrany dat, práce s uživateli těchto dat, jejich vzdělávání a dlouhodobě koncipovaná technologická a procesní řešení.

V materiálech vaší společnosti, jsem si také přečetl, že zabezpečení dat vyžaduje nové myšlení. Můžete to více konkretizovat?

Nové myšlení, které v našich materiálech používáme, není jen „buzzwordem“, termínem, který by byl marketingově umělý a přitom obsahově vyprázdněný. V ATOSu věříme, že zabezpečení dat, bezpečnost informací, kybernetická bezpečnost není pouze technologický problém, ale především otázka přístupu a vnímání dat a informací jako hodnoty, kterou společnosti, jednotlivci i vlády chtějí a potřebují chránit, podobně jako například chrání platidla, či komodity. Změna myšlení celé společnosti a v první řadě odpovědných osob je proces dlouhodobý, trvající řádově roky. Velké společnosti jako ATOS na tuto změnu reagují a jsou schopny ji uchopit systémově. ■

Kontakt: Tomáš Hlavsa,
tomas.hlavsa@atos.net,
+420 604 290 196