Kybernetické útoky v energetice   
  
**V jedné z předchozích analýz se Česko v datech zabývalo energetikou a výrobou energie v České republice. Řeč přišla i na tzv. inteligentní rozvodné sítě – tedy ty, které umožňují regulovat výrobu a spotřebu elektrické energie v reálném čase a obousměrně komunikovat mezi výrobními zdroji a spotřebiči nebo spotřebiteli – a spolu s nimi i nutnost jejich efektivního zabezpečení. Je ale hrozba útoku na energetické sítě skutečná? Co může znamenat pro koncového odběratele? A jak se proti útokům bráníme v Česku? Podívejte se na názory odborníků a případy z minulosti, které pro vás Česko v datech shromáždilo.**  
Odpověď na první otázku je jednoduchá a zároveň poněkud znepokojující. Ano, s kybernetickými útoky na společnosti energetického sektoru se dnes odborníci už nesetkávají jen v rovině teoretických úvah, ale i ve skutečnosti. A přizpůsobovat tomu samozřejmě musí i svou práci, stejně jako u jiných útoku, i u hrozeb pro energetické sítě je třeba identifikovat případná rizika a připravit scénáře pro minimalizaci případných škod. „*V současnosti už v podstatě neexistuje složitější energetický systém, který by byl řízený bez využití informačních technologií. Zejména u ovládacích systémů klíčových prvků sice stále existuje velká snaha o striktní oddělení od veřejné sítě, ne vždy je to z provozních důvodů možné,“* vysvětluje **Libor Šup, Solutions Architect ze společnosti Unicorn Systems**.  
  
Kybernetickým útokem v energetice se míní situace, kdy se hacker nebo skupina hackerů pokusí získat přístup ke klíčovým informacím či prvkům infrastruktury (např. elektrárnám, rozvodným soustavám či řídícím centrům), s cílem ovládat je nebo do nich nahrát škodlivý kód, který bude vykonávat určené příkazy. Motivací pro útočníky může být osobní zisk, zničení vybraného cíle, vyvolání paniky a napáchání dodatečných škod nebo prostě „jen“ chuť ukázat, že něco takového dokáží.

*„Podle statistik britského serveru hackmageddon.com byl v roce 2015 celkový počet kybernetických útoků výrazně vyšší než v roce předchozím, a to i navzdory neustále se vyvíjející obraně proti podobným případům. Zhruba za pětinou zaznamenaných útoků stáli nejrůznější aktivisté a skupiny, 10 % útoků je dílem špionáže a jen asi 24 případů z tisíce pak připadá na tzv. kybernetickou válku. Na průmyslové podniky včetně oblasti energetiky mířila celá čtvrtina útoků, daleko za nimi jsou pak vlády, zdravotnická zařízení nebo finanční instituce,”* přibližuje strukturu současné kyberkriminality **Zuzana Lhotáková, Marketing manager SAS Institute ČR.***„Útočníky můžou být jednotlivci, ale i organizované skupiny aktivistů, teroristé, vládní organizace nebo armáda. Mezi takové skupiny patří například Energetic Bear, která je podle zpráv z několika nezávislých zdrojů zapojena do kybernetické špionáže v oblasti energetiky a škodlivý software z jejich dílny – Havex – je rozšířen po celém světě. Havex se v současnosti nezaměřuje jen na kybernetickou špionáž, ale je schopen také sabotovat infikované systémy. To je velmi závažné zjištění, protože jeho cílem jsou primárně SCADA (Supervisory Control and Data Acquisition) systémy využívané energetickými společnostmi. Energetic Bear mají nejpravděpodobněji sídlo ve východní Evropě a jejich malware se objevil mimo jiné i v Česku. Z činnosti skupiny je patrné, že pracuje v běžném pracovním týdnu, a dá se tedy usuzovat, že se nejedná o nadšence, ale členy nějaké organizace, která bude mít silné finanční zázemí,“* dodává **Libor Šup z Unicorn Systems**.  
  
--  
  
Kde už hackeři na energetické systémy zaútočili?  
Vybrali jsme pro vás největší případy útoků na energetické sítě poslední doby.   
  
**Zpoždění při spouštění íránské jaderné elektrárny**Už v roce 2010 byl zaznamenán kybernetický útok, který měl za úkol oddálit nebo zastavit spuštění jaderné elektrárny v Iránu. Cílem ochromení tehdy nebyla samotná jaderná elektrárna, ale závod na obohacování uranu. Červ Stuxnet vyřadil z činnosti a následně zničil několik stovek centrifug na obohacování uranu tím, že změnil frekvenci jejich otáček. Nejprve je roztočil nad povolenou hranici a poté jejich otáčky naopak snížil na velmi pomalé. Tím způsobil finanční ztráty i zpoždění při zprovoznění samotné elektrárny. Vzhledem k architektonické složitosti tohoto červa se muselo jednat o experty s obrovským finančním potenciálem. Stuxnet je natolik kvalitní a modulární systém, že je možné jej u průmyslových systémů využít pro téměř libovolnou podobnou činnost. I proto byly z útoku podezřívány tajné služby USA a Izraele, avšak bez jasných důkazů.  
  
**Převzetí kontroly nad vodním dílem v USA**Pravděpodobně jako odvetu za útok proti jaderné elektrárně v roce 2013 podnikla íránská skupina SOBH Cyber Jihad, která se k útoku sama přihlásila, úspěšný kybernetický útok na malou přehradu (přesněji větší stavidlo) poblíž New Yorku. Podařilo se jim na krátkou dobu převzít kontrolu nad ovládacím zařízením a i když se tentokrát jednalo o malé vodní dílo o výšce několika metrů, i tento útok ukázal možné následky plynoucí z nedostatečného zabezpečení.  
**Únik informací v Jižní Koreji**V prosinci 2014 došlo k útoku na servery společnosti Korea Hydro & Nuclear Power, která v Jižní Koreji provozuje několik jaderných elektráren a hydroelektráren. Došlo k úniku dat, která ovšem podle vyjádření společnosti nepatřila mezi klíčová. Podobné informace však mohou být cenné při plánování dalšího útoku. Možná spojitost s KLDR nebyla potvrzena ani vyvrácena.  
  
**Masivní výpadek dodávky elektrického proudu na Ukrajině**V prosinci roku 2015 došlo k rozsáhlému výpadku dodávek elektrické energie v Ivanofrankivské oblasti na Ukrajině. Bez elektřiny tehdy zůstalo po dobu několika hodin až 700 tisíc lidí. Z následných analýz útoku vyplynulo, že se nejednalo o náhodný výpadek, ale koordinovanou součinnost skupiny hackerů. Ti pomocí trojského koně BlackEnergy pronikli do jednotlivých komponent distribučních sítí a následně ji poškodili nebo ochromili. Kromě klasických funkcí destruktivního malware (odstranění systémových souborů, které znemožní spustit systém) se tato varianta speciálně zaměřila na sabotáže v průmyslových systémech. Jednalo se tedy o konkrétní aplikaci běžného malware pro potřeby útoků na podobné cíle. I když konkrétní útočník nebyl odhalen (spekuluje se o jeho napojení na ruské vládní složky), jedná se o první jasně potvrzený útok na rozvodnou elektrickou síť v tomto rozsahu. Podobný trojský kůň byl využit i pro útok na ukrajinská média po volbách nedlouho předtím a spekulovalo se i o hrozbě pro kyjevské letiště, kterou se však údajně podařilo včas zastavit.  
  
--  
*„Kybernetické útoky bychom neměli řadit jenom jako problematiku IT. Pro sofistikovaný útok totiž útočník používá více různých prostředků, přičemž nejčastěji využívá psychologický aspekt zranitelnosti uživatele. Oklamáním uživatele totiž útočník umístí do vnitřní sítě organizace falešnou bránu, malware, která pak simuluje interního uživatele. Pak už bezpečnostní brány, firewally, nerozliší komunikace útočníka pod ukradenou identitou oproti oprávněnému uživateli. Ale i proti takovýmto útokům se lze bránit pojetím bezpečnosti multidisciplinárně,”* vysvětluje **Adrian Demeter, senior manažer Deloitte Security**.

**Kybernetické útoky a český spotřebitel**Běžnému spotřebiteli nebo firmě se podobné útoky mohou zdát vzdálené a málo pravděpodobné. Ale s nástupem tzv. ‚chytrých domácností‘ a internetu věcí se začíná riziko kybernetických útoků přibližovat i jim. Reálná je například situace, kdy útočník přepíše údaje na elektroměru se vzdálenou správou nebo vzdáleně zapne v domácnosti spotřebič – například topení – s cílem uměle navyšovat spotřebu energií. Na podobném principu může fungovat převzetí řízení jaderné elektrárny, regulace výpustě přehrady nebo manipulace s přenosovou soustavou či zásobníky plynu.  
  
V současnosti v ČR dochází k pomalému posunu ve vnímání kybernetických hrozeb nejen pro energetický sektor. Děje se tak na základě platného kybernetického či krizového zákona, případně z vůle jednotlivých subjektů. V neposlední řadě probíhají kybernetická cvičení, která pomáhají hledat možná rizika a nabízet jejich řešení – například v říjnu 2015 proběhlo v Brně pod záštitou Národního centra kybernetické bezpečnosti cvičení simulující útok na elektrárnu i obranu před ním, ve kterém proti sobě stály týmy „útočníků“ a „obránců“.

**O projektu Česko v datech**

Ambicí projektu Česko v datech je vyhledávat témata, která jsou přitažlivá, zajímavá nebo důležitá pro celou společnost, ale jejichž zpracování vyžaduje pokročilé datové nástroje. Chce objevovat souvislosti, které se v datech skrývají, a potvrdit či vyvrátit tvrzení, která se v české společnosti tradují, ale bez práce s rozsáhlými daty jim chybí důkaz. Partnery projektu jsou společnosti SAS Česká republika,​ Deloitte, Unicorn a DataSpring, ​které poskytly svá řešení pro zpracování a vizualizaci dat. Spolu s nimi se na projektu podílí i agentura DARK SIDE.