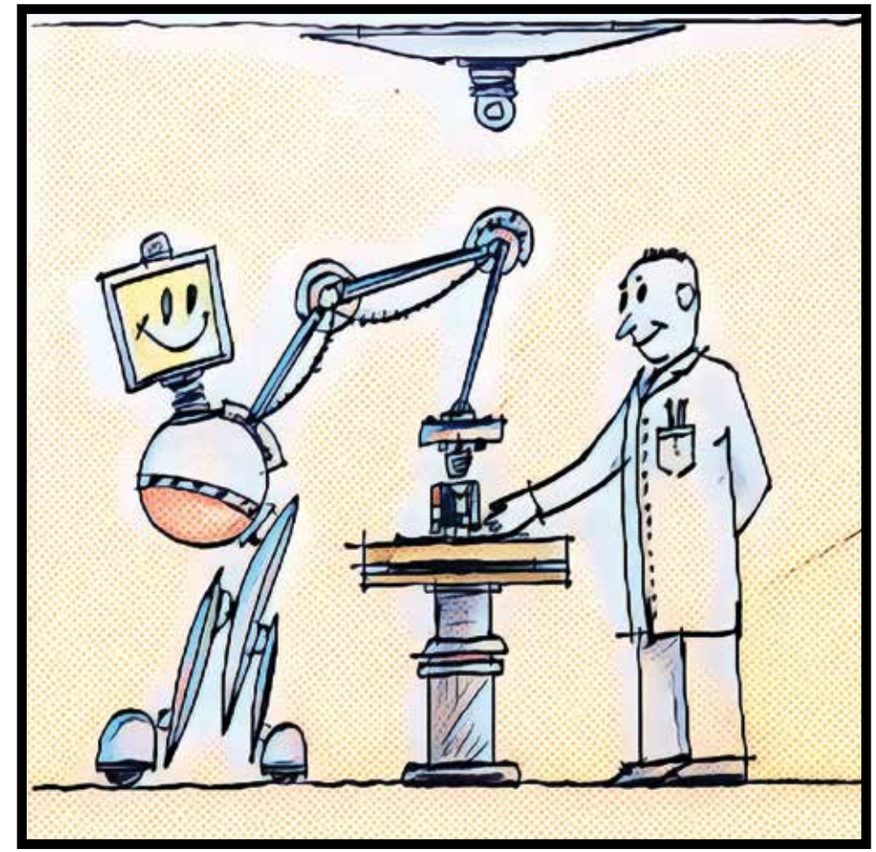
BEZPEČÍ SYNOPCITY
OBRANA PŘED KYBERZLOČINEM



Kresba Michal Postránecký

„Museli jsme vymyslet technologii, která by zajistila bezpečnost těchto obchodů na stejné úrovni, na jakou jsme zvyklí z bankovnictví. A tak jsme přišli s technologií elektronického podpisu, která bezpečnost těchto transakcí umožňovala.“

Petr Budiš, I. CA

CHYTRÁ MĚSTA SE BRÁNÍ PŘED KYBERLUPIČI

Kyberútoky na desítky tisíc počítačů současně jsou již skutečností. Jak se jim bránit?

Grid nebyl k zastavení. Jen co jsem se zmínil, že bych se rád dozvěděl něco o boji proti kyberzločinu v Synopcity, hned rozjel akci. Minutu někam ***ze sebe*** skypoval a volal a už mě táhl na právě domluvenou schůzku.

„Kyberzločin, to je moje! Právě včera jsem o tom napsal článek do RobotiaNews. Nečetl jsi to?“ začne švitořit a táhne mě přes virtuální přechod. Tak nepozorně, že nás málem porazí maglevtaxi, které právě neslyšně, ale o to svižněji proplouvá silnicí půl metru nad vozovkou.

„Jdeme za Petrem Budišem, to je hlavní bezpečnostní poradce Synopcity. A znám se s ním, protože on mé články čte a líbí se mu,“ podívá se na mě trochu vyčítavě.

„Jo, a to víš, že první počítačový zločin byl spáchán už v roce 1820?“ poučí mě Grid před dalším přechodem, kde se už naštěstí rozhlédne. *„Joseph Marie Jacquard tehdy sestrojil první tkalcovský stav, který se programoval pomocí děrných štítků. A víš, co udělali dělníci v té francouzské továrně, kde ho nainstaloval?“* zastaví se na pětníku a zkoumavě na mě pohlédne.

„Rozflákali ho…?“ tipnu si nesměle.

„Rozbili. Přesně tak. Takový technický skvost! Co by za něj dnes SynopMuzeum dalo... No jo, lidi... Tohle by roboti nikdy neudělali, jako že je Isaac Asimov nade mnou!“

Největší kyberútok v dějinách zasáhl 74 států

O 6000 procent (a není to bohužel překlep) vzrostl podle nejnovějších údajů IBM v roce 2016 počet ransomwarových útoků ve světě. Nový fenomén vyděračských ataků, které žádají výkupné za odblokování vašeho počítače a vrácení ukradených dat, vydělal jen loni více než miliardu dolarů. A počet obětí stoupá exponenciální křivkou každý den. Letošní čísla tak budou zřejmě ještě děsivější.

Bitevní pole. Globální ransomwarový kyberútok z loňského května ochromil 45 000 počítačů v 74 zemích světa

66 VŠEDNÍCH ZÁZRAKŮ V SYNOPCITY

Palantir předvídá zločiny

Vylepšený software ***Palantir***, nazvaný podle vidoucích kamenů z Pána Prstenů, se stal základem technologie vybavené umělou inteligencí. Ta v Synopcity předvídá kriminalitu. Umí například odhalit připravované teroristické útoky, zločinná spiknutí či trasy velkých zásilek drog. ***Palantir*** gigabyty sebraných informací zpracovává a s pomocí aplikace XKeyscore analyzuje. Například získá všechny IP adresy z Moskvy a Teheránu, ze kterých odešly maily na konkrétní webové adresy, nebo přes které byl veden Skype hovor. Získaná data Palantir zanalyzuje, odhalí další spojení mezi adresami a je schopen i graficky zmapovat polohu podezřelých.

Dosud největší globální kybernetický útok zasahuje letos v květnu počítače v 74 zemích světa. Kyberlupiči podle britského Guardianu paralyzují nejméně 45 tisíc přístrojů vyděračským softwarem. Za jejich odblokování požadují neznámí pachatelé výkupné v hodnotě 1 bitcoinu, což je v aktuálním přepočtu skoro 90 tisíc korun.. “Jde o jeden z největších globálních ransomwarových útoků, jaký kybernetická komunita kdy viděla,” komentuje pro Reuters útok nevídaných rozměrů Rich Barger, ředitel výzkumu kybernetických hrozeb americké společnosti Splunk.

Dodnes není zcela jasné, kdo za útoky stojí. Podle bezpečnostních expertů byl použit hackerský nástroj, který vyvinula americká Národní bezpečnostní agentura (NSA). Na internet se dostal díky hackerské skupině Shadow Brokers, která od loňského léta zveřejňuje uniklá špionážní data i jména softwarových špionů všemocné NSA.

Bankovní sektor zajímá kyberzločince stále více,“ říká Ing. Petr Budiš, Ph.D. MBA

Klávesnice místo baseballové pálky

Česko se stalo podle společnosti ESET devátou nejvíce postiženou zemí tohoto masivního ataku. Taková je realita. Obětí kyberútoku na vaše osobní data či

BEZPEČÍ SYNOPCITY

Robopsi patrolují na hranicích

Robopes, nebo též ***BigDog*** společnosti Boston Dynamics, hlídá území na přirozených hranicích Synopcity. Sto deseti kilový, metr vysoký strážce je vybaven 16 hydraulickými klouby, které dokážou recyklovat energii z jednoho kroku do druhého. Nejnovější model na vodíkový pohon dokáže vystoupat svahy strmé až 35 stupňů, unese 150 kilo zátěže, prochází lesním terénem, sněhem, vodou i sutinami.

Palubní počítač řídí jeho pohyb i senzory a ovládá komunikaci. Senzory pohybu s gyroskopem citlivě dirigují pohyby všech kloubů a systém stereofonního vidění z něj dělá nepostradatelného pomocníka ***robohlídek*** strážících bezpečí Synopcity.

Jednoduché a proto účinné. Technologie I.CA stály u zrodu bezpečného internetového bankovnictví v ČR

bankovní účty se stanete v éře digitální revoluce statisticky častěji, než jaká je šance, že vás přepadne na zšeřelé ulici zakuklený gangster. A oloupí pěkně „postaru". Bohužel? Bohudík?

„21. století přineslo prudký rozvoj bankovních služeb poskytovaných elektronickými médii. Současně s tím se o bankovní sektor začali čím dál více zajímat kyberzločinci," vysvětluje Ing. Petr Budiš, Ph.D. MBA, předseda představenstva První certifikační autority (I.CA) a hlavní bezpečnostní poradce Synopcity. „Jejich útoky jsou stále propracovanější a dnes se snadno můžete stát obětí virtuální krádeže kdekoli v dosahu internetového připojení. Než třeba v obchodním centru s Wi-Fi zaplatíte kartou za nákup, může být váš bankovní účet úspěšně ‚vybílen'."

Na konci minulého roku například postihla kybernetická loupež 20 tisíc běžných účtů britské Tesco Bank. A domníváte-li se, že pokud nejste boháči, riziko se vás netýká, podle mluvčího banky šlo u jednotlivých napadených účtů právě o „relativně nízké částky".

66 VŠEDNÍCH ZÁZRAKŮ V SYNOPCITY

Medoosa zmrazí vetřelce v letu

Kosmodromy, vojenská zařízení, ale i vládní budovy v Synopcity chrání protidronový systém ***Medoosa*** (Mobilní Elektronický Detekční Obranný a Ochranný Systém AntiUAV), vyvinutý českou firmou Elias Palme. Toto mobilní zařízení je schopno detekovat nepřátelský bojový či špionážní dron od velikosti 50 centimetrů i na vzdálenost 10 kilometrů v akčním rádiu 360 stupňů až do výšky 10 kilometrů. To vše v kteroukoli denní i noční dobu a při jakémkoliv počasí. ***„Medoosa navíc umí rozlišit vlastní a cizí zařízení a v nejkratším čase vytvořit velmi úzký koridor o rozsahu 16 - 19 úhlových stupňů. A v něm zachycený UAV znehybnit. Tím získá ostraha čas k reakci,"*** vysvětluje Ing. Dalibor Miketa, jeden z tvůrců ***Medoosy***.

ePodpis proti podvodníkům

Projekt I.CA vznikl v době, kdy se už začaly i v Česku objevovat první, byť proti dnešku více než nesmělé útoky hackerů. Píšou se „devadesátky" a elektronická komunikace se začíná prosazovat do podnikání. Navíc startuje kupónová privatizace a držitelé akcií s nimi začínají obchodovat. Proto je třeba vymyslet systém, v němž si obchodníci budou schopni rychle a především bezpečně předávat informace a provádět online obchody často stamilionových hodnot.

V chytrých městech budeme muset za pohodlí a komfort obětovat část svého soukromí

BEZPEČÍ SYNOPCITY

Roboponorky číhají pod hladinou

Neslyšně, ale o to bedlivěji hlídají hladinu moře i jeho hlubiny u břehů Synopcity bezpilotní roboponorky. Mají řadu výhod. Mohou být menší a tudíž hůře zachytitelné sonary. A nemusí řešit otázku doplňování zásob nebo vynořování pro načerpání kyslíku. První typem robotické ponorky ve službách Synopcity byl ***Proteus*** od americké firmy Columbia Group, pojmenovaný podle řeckého boha moře. Kromě strážních misí je schopna i nepozorovaně vylodit sedmičlennou bojovou jednotku. Úctyhodné parametry má i miniaturní autonomní ponorka ***Spray Glinder***. Je dlouhá jen 213 cm a má 20 centimetrů v průměru. Na moři však dokáže strávit až 6 měsíců a urazit během nich více než 4 800 kilometrů.

„A protože se tyto obchody uskutečňovaly ve vysokých finančních objemech, hrozilo velké riziko podvodů. Museli jsme vymyslet technologii, která by zajistila bezpečnost těchto obchodů na stejné úrovni, na jakou jsme zvyklí z bankovnictví. A tak jsme přišli s technologií elektronického podpisu, která bezpečnost těchto transakcí umožňovala," vysvětluje Ing. Petr Budiš.

A je to právě elektronický podpis, u jehož zrodu a rozšíření I.CA stála, který je dodnes jednou z nejúčinnějších zbraní proti kyberútokům. Epodpis totiž nade vši pochybnost identifikuje totožnost odesílatele. A virtuální časové razítko, další z produktů První certifikační autority, hojně používaných po celé Evropě i v zámoří, zase dává elektronickým dokumentům – kromě puncu pravosti – i nezpochybnitelné ukotvení v čase. Největšími zákazníky I.CA jsou proto banky a orgány veřejné správy, zejména ministerstva. Elektronické bankovnictví je dnes standardní službou a klíčovým požadavkem bank i majitelů účtů je vysoká bezpečnost při zachování uživatelského komfortu.

„My jsme v podstatě ta třetí, důvěryhodná strana v bezpečné elektronické komunikaci jiných dvou subjektů. Důraz je třeba klást právě na onu důvěryhodnost. Proto u nás věnujeme bezpečnosti velkou pozornost. Bezpečnostní požadavky na instituce, poskytující certifikační služby, podléhají velice tvrdým normám," vysvětluje Petr Budiš.

Nezvěte hackery do svých IT dveří!

Rozlišit podvodný mail – velmi často nenápadný předvoj ransomwarového útoku – od legitimní zprávy vaší banky zase není tak těžké. Stačí dávat pozor a respektovat bezpečnostní pravidla.

„Zpráva od banky by vždy měla být elektronicky podepsaná, a ne anonymní," říká Petr Budiš. Je pak zcela zbytečnou neopatrností otevírat jakékoli podezřelé e-mailové

Railguny vymažou z oblohy cokoliv

A teď trochu silnější kalibr. Obranu Synopcity zajišťují (mimo jiné) baterie ***railgunů,*** elektromagnetických děl na palubách robotických lodí i na pevnině. Dokáží vystřelit speciálně tvarované projektily pomocí silného elektromagnetického pole (využívající tzv. Lorentzovou sílu) rychlostí Mach 7, což je 8400 km/h. ***„Není žádná věc na obloze, která by mohla zásah přežít,"*** říká kontraadmirál Matthew Klunder,

bývalý šéf námořního výzkumu Naval Research, který je dnes velitelem námořních sil v Synopcity. Má asi pravdu, protože rychlost projektilu je tak velká, že při kontaktu s atomy vzduchu vytrhává elektrony z atomových obalů a vytváří plazmu. ***Railguny*** dokáží ničit hladinové, pozemní, vzdušné i balistické cíle přímou i nepřímou palbou. Naštěstí to zatím nebylo zapotřebí.

Pohodlné bankovní produkty zvyšují nebezpečí kyberútoku

zprávy nebo dokonce jejich přílohy. Ty mohou obsahovat různý škodlivý software, který útočníkovi pomůže dostat se k vašim důležitým datům a ovládnout váš počítač. Citlivé informace se navíc mohou hackeři pokusit získat i mimo kyberprostor, například po telefonu.

Třeba loni přišel o 40 milionů eur německý koncern Leoni. Stal se obětí spear phishingu – sofistikovanému útoku, cílícího právě na největší bezpečnostní slabinu každého systému – člověka. Finanční ředitelka rumunské pobočky byla oklamána a sama provedla převod peněz v domnění, že vykonává instrukce vedení.

Vesmírné bombardéry v záloze

Vesmírný letoun, který může být osazen jadernými zbraněmi a je schopný do dvou hodin od vzletu zničit jakékoliv místo na planetě, je zdejší zbraní „poslední možnosti". ***"Bombardér odstartuje z domovského letiště podobně jako obyčejné letadlo. Poté zamíří do vnějšího vesmíru, odkud shodí jaderné hlavice a vrátí se zpět na základnu,"*** popsal unikátní stroj podplukovník Petr Kovalewski, který má v Synopcity tyto stroje pod svým velením. Letoun o váze 200 tun při vzletu nejdříve spálí kapalné pohonné hmoty, poté přejde na kyslíkové palivo. To mu udělí „únikovou" nadzvukovou rychlost, s níž je schopen vystoupat na nízký orbit.

„Nezapomínejte, že ani po telefonu nejste povinni sdělovat nějaké informace jen proto, že se někdo ptá. Když vám někdo cizí zazvoní u dveří, taky ho hned nepozvete dál. Tak proč byste otevírali pomyslné dveře v IT komunikaci? Úspěch hackerů totiž závisí na slabinách těch, na které útočí. A klíčová je slabost zevnitř," říká Andor Šándor, bezpečnostní poradce a bývalý náčelník Vojenské zpravodajské služby. Ochrana před kybernetickým zločinem tak musí být systémová, ale nesmíme zapomínat ani na odpovědnost jednotlivce. A to nejen klienta, ale každého, kdo je do procesu zapojen.

„Je přirozené, že chceme nakládat se svými penězi co nejpohodlněji," souhlasí Petr Budiš. „Pokud ale budeme nadále vytvářet v bankovním sektoru poptávku především po pohodlných produktech, bude jejich bezpečnostní stránka trpět."

V USA zaútočili pomocí chytrých spotřebičů

I tohle vypadá jako zpráva ze sci-fi magazínu, ale bohužel také není. Hackeři provedli loni v říjnu v USA útok pomocí chytrých spotřebičů připojených k internetu. Jeden z prvních zaznamenaných ataků pomocí tzv. internetu věcí (IoT) dostal mimo provoz servery Twitteru, Spotify, PayPalu a dalších významných firem.

Hackeři takzvaný DDoS útok zosnovali tak, že se na dálku zmocnili ovládání tisíců smart spotřebičů – dětských chůviček, kamer, lampiček či wi-fi routerů – připojených k internetu.

Kyber napadení potvrdila listu New York Times společnost Dyn, monitorující a směrující datové toky. Výpadky začaly již ráno na východním pobřeží USA a během dne se ve třech vlnách šířily směrem na západ. Jak tedy vidno, s profi ochranou (nejen) dat, ale i samotného přístupu k našim počítačům zvenčí už asi opravdu není radno otálet.

Inteligentní helma s 3D projekcí

Helmy vybavené ***rozšířenou realitou*** a vesty s elektricky vodivými nitěmi a bezdrátovým dobíjením vyvinula pro bezpečí vojáků Synopcity britská zbrojařská firma BAE Systems. Neprůstřelná vesta ***Spine*** je vybavena hlavní řídicí jednotkou pro distribuci energie a dat. Má v sobě zabudovaných 8 konektorů, do kterých může voják zapojit různá podpůrná zařízení. Kevlarová helma má průhledový displej, datové připojení a elektro-optické senzory. Na displeji se vojákovi zobrazují data z bojiště i informace o vlastních a nepřátelských jednotkách. Přilba je vybavena i kamerou pro noční vidění.

3 nejzákeřnější kyberútočníci

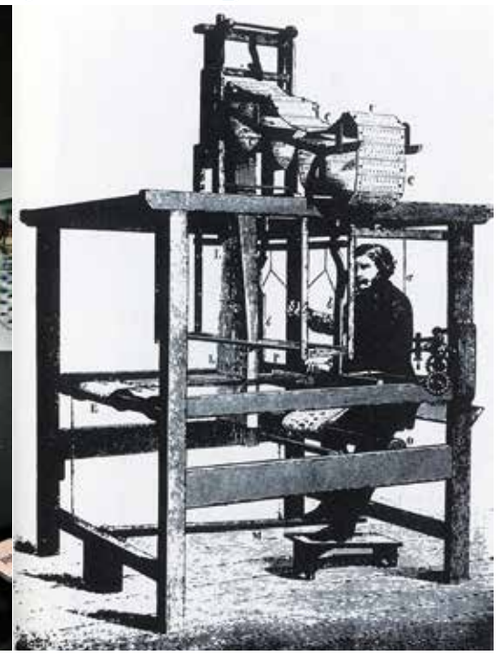
Seznam nejnebezpečnějších kybernetických útoků sestavil Artur Kan, specialista společnosti Flowmon Networks. tři z nich vybíráme.

- **Farmaření: *Pavoučí síť.*** Cílem farmaření je přesměrovat oběť na škodlivou webovou stránku, která vypadá jako originální. Možností, jak toho docílit a dostat uživatele na podvodný server, je celá řada. Ta nejnebezpečnější, která nevyžaduje žádný přístup nebo kontrolu nad koncovou stanicí uživatele, využívá falešnou DNS (Domain Name Server).
- **Botnet: *Hitchcockovi ptáci.*** Botnet je synonymum pro velké množství kompromitovaných počítačů, které pracují jako tým. Hlavním nebezpečím je zde množství. Odtud analogie se slavným dílem režiséra Alfreda Hitchcocka. Botnety jsou jednoduché kódy primárně vytvářené pro DDoS útoky, šíření spamu nebo nejrůznějších typů malwaru.
- **Malware: *Tygr vyčkává v záloze.*** Tyto typy malwaru jsou naprogramovány tak, aby prováděly širokou škálu úkolů: Od otevírání zadních vrátek k systémům nebo hledání informací odhalujících zranitelnosti přes způsobení pádu aplikace či celého systému až po smazání dat.

Mikrovlnná kamera vidí skrze zdi

Vojenští výzkumníci ze Synopcity nedávno úspěšně dovršili vývoj ***mikrovlnné kamery***, která dokáže zachytit detailní 3D obraz skrz zeď. Aby byly senzory schopny zachytit obraz při tak dlouhých vlnových délkách, musí pokrýt velmi široký výřez v dostatečné hustotě. Standardní radar k tomu používá stovky tisíc senzorů. Namísto rozmístění elektroniky přes celou plochu zařízení výzkumníci dokázali elektroniku vměstnat na plochu o rozměrech pouhých 25 x 25 cm. Použili přitom velké pasivní reflektory, aby soustředili energii do malé oblasti. Cílem tohoto postupu je vyšší kvalita výsledného obrazu. ***Mikrovlnné kamery*** budou účinnou zbraní při prevenci kriminality či v boji proti terorismu.

Kyberzločiny začaly píšťalkou, dnes vydělávají miliardy dolarů



První tkalcovský stroj Josepha-Marie Jacquarda se zařízením na děrné štítky

1820

Rozčílení dělníci rozbíjejí tkalcovský stav Josepha-Marie Jacquarda ve Francii. První tkalcovský stroj, který je **vybaven automatickým zařízením na děrné štítky**, umožňujícím opakovat některé jednoduché operace. Dělníci se bojí, že je automat připraví o práci. Dějiny počítačového zločinu právě odstartovaly.

1971

John Draper, americký veterán z Vietnamu, zjišťuje, že píšťalka přikládaná jako dárek ke krabicím s cereáliemi Cap´n Crunch (Kapitán Křup) dokáže vyloudit tón o frekvenci 2 600 Hz. A přesně tentýž tón používají americké telefonní ústředny pro vzájemnou komunikaci. Se „zázračnou" píšťalkou za pár centů se dá **hvízdáním do sluchátka přepojit z místního hovoru,**

John Draper a jeho „zázračná" telefonní píšťalka

který je zdarma, na placený dálkový hovor. Bez jediného centu vhozeného do automatu. V některých státech USA se v té době prý „odpískala" až čtvrtina dálkových hovorů.

1973

První skutečný zločin spáchaný pomocí počítače. Bankovní úředník z Dime Savings Bank, který ho obsluhuje a zná procesy v bance, **dokáže na svůj úč**et převést 1,5 milionu dolarů. Banka přitom na nic nepřijde a úředník je zatčen až poté, co policie vyšetřuje, kde vzal úředník peníze na nelegální hazard.

1981

Ian Murphy na dálku **změnil algoritmus výpočtu tarifů v počítačích** telekomunikační společnosti AT&T, které pak účtovaly i ve špičce snížené sazby. Již rok poté dosahují v USA počítačové podvody takového rozměru, že je nutno boj s nimi převést do zodpovědnosti US Secret Service.

1988

Morrisův červ – jeden z prvních rozpoznaných červů, který ovlivnil globalizující se kybernetickou infrastrukturu světa – se v USA začíná šířit počítačovými sítěmi. Počítače zpomaluje tak, aby byly nepoužitelné. Červ je dílem Roberta Tappana Morrise, který tvrdí, že se pokouší zjistit, jak velký je internet. **Američan se stává prvním člověkem v dějinách odsouzeným podle zákona o počítačových podvodech**. Dostává nepodmíněně 3 roky vězení, 400 hodin veřejně prospěšných prací a pokutu 10 00 dolarů. Dnes je Morris profesorem na Massachusettském technologickém institutu v USA.

Z hackera profesorem. Robert T. Morris, odsouzený jako první v dějinách za hacking, je dnes profesorem na Massachusettském technologickém institutu v USA.

1993

Hacker Kevin Poulsen se svými přáteli pomocí jednoduchého útoku **zablokuje všechny telefonní hovory** do rozhlasové stanice Kiis FM v Los Angeles během velké rozhlasové soutěže. Kromě svých telefonních linek. **Díky tomu vyhrají – jako jediní volající – dva automobily Porsche, několik dovolených a prémii 20 tisíc dolarů.** Poulsen je odsouzen k pěti letům vězení. V rozhovorech pro média tvrdí, že mu šlo o pomstu na federálních úřadech. Hackeři prý odhalili odposlouchávání ambasád Číny, Izraele a Jižní Afriky americkými tajnými službami.

1995

Skupina útočníků kolem ruského hackera Vladimira Levina **odcizuje z Citibank 10 milionů dolarů.** Během několika hodin je dokáže vybrat z bank ve Finsku a v Izraeli. Policie je však rovněž rychlá a všechny peníze z lupu (kromě půlmilionu dolarů) zajišťuje.

2000

Hackeři z Ruska stahují osobní údaje a čísla kreditních karet klientů hudebního obchodu Universe. **Následně požadují 100 tisíc dolarů za to, že údaje nezveřejní.** Obchod odmítne a útočníci svoji hrozbu splní. Universe následně nabídne bezpečnostnímu expertovi Barrymu Schlossbergovi 1,4 milionu dolarů, když dokáže ruské útočníky vypátrat, vylákat do USA a předat policii. To se nakonec povede díky pomoci FBI, která založí v Seattlu falešnou bezpečnostní start-upovou firmu. A těm, které potřebuje dostat na americké území, nabízí atraktivní práci. Postup několikrát zopakuje i v dalších případech počítačové kriminality, než se tato lest prozradí.

2006

Zpráva FBI za rok 2005 konstatuje, že příjmy z kybernetických zločinů svým celosvětovým objemem **překročily** příjmy obchodu s narkotiky.

V témže roce je NASA nucena **zablokovat e-maily s přílohami předtím, než odstartuje raketoplán Atlantis** ze strachu, aby nebyly ukradeny. Časopis Business Week oznamuje, že plány nejnovějších amerických kosmických nosičů byly získány počítačovými lupiči.

Vir „Rudý říjen" řádil v počítačích na celém světě

2007

Soukromý e-mailový účet ministra obrany USA Roberta M. Gatese je hacknutý neznámými vetřelci. Jde o součást většího počtu útoků na síť Pentagonu v tomto roce. Čínské ministerstvo pro bezpečnost státu zase zveřejňuje informaci, že **hackeři z Tchaj-wanu a USA ukradli informace** z klíčových oblastí čínské politiky, ekonomiky a obrany.

2009

Hackeři **napadají izraelskou internetovou infrastrukturu** během vojenské ofenzívy v pásmu Gazy. Útok, který je zaměřen na vládní webové stránky, je proveden pomocí nejméně 5 milionů počítačů. Izraelští úředníci věří, že za útokem stojí zločinecká organizace se základnou na území bývalého SSSR, placená Hamásem či Hizballáhem.

2010

Stuxnet, nebezpečný malware určený k interferenci s průmyslovými řídicími systémy Siemens, je objeven v Íránu, Indonésii i v dalších zemích. Objevují se spekulace, že **jde o americkou vládní počítačovou zbraň**, zacílenou na íránský jaderný program.

2012

Ruská firma Kaspersky Lab ohlašuje **celosvětový počítačový útok nazvaný „Rudý říjen"**. Hackeři shromažďují informace díky chybám v zabezpečení programů Microsoft Word a Excel. Hlavními cíli útoku jsou země Východní Evropy, bývalý SSSR a Střední Asie. Virus shromažďuje informace z velvyslanectví, výzkumných firem, vojenských zařízení i z jaderných infrastruktur.

Návratnost kyberzločinu je podle nedávné studie společnosti Trustwave až na hranici 1425 procent. Za investovaných 5900 dolarů je možné získat zpět 84 100 dolarů

2016

Dosud největší globální kybernetický útok v dějinách zasahuje v květnu počítače v 74 zemích světa. **Kyberlupiči paralyzují nejméně 45 tisíc přístrojů vyděračským softwarem**. Za jejich odblokování požadují neznámí pachatelé výkupné v hodnotě 1 bitcoinu, což je v aktuálním přepočtu skoro 90 tisíc korun.

(Zdroj: www.nato.int, Tomáš Přibyl, Computerworld)

POSEL CHYTRÉ BUDOUCNOSTI
CHYTRÝ LUXUS ZA KUS SOUKROMÍ?

„Elektronický podpis má budoucnost," říká Petr Budiš

Prvotní úvaha říká, že je dnes už možné prakticky všechno, co si vůbec dovedeme představit. Omezuje nás pouze to, co si představit umíme a co neumíme. Člověk je navíc svázán konvencemi a zvyky, které nerad opouští. Další rozvoj informačních technologií, ale i technologií obecně, začíná narážet na psychologickou a sociální bariéru.

Ing. Petr Budiš, Ph. D., MBA
generální ředitel První certifikační autority, a. s.

Ve Smart cities změníme své návyky

Vezměme si příklad autonomního řízení osobních automobilů. Pokud pomineme aspekt zodpovědnosti takového „zařízení" za bezpečnost přepravy pasažérů a za bezpečnost jejich okolí, musíme se zamyslet nad tím, že pustíme volant, přestaneme šlapat na pedály a uvěříme tomu, že auto pojede bezpečně a rychle z bodu A do bodu B. Už ho neovládáme, neřídíme. Za čas navíc zapomeneme, jak se řídí, protože to už nebudeme potřebovat umět.

Co tedy budeme chtít a co budeme potřebovat? V moderních městech to bude podobné. Dnes máme svoje rutiny. Ty se budou měnit. Otázkou je, jak rychle a jakým směrem. Určujícím pro další vývoj tedy primárně není vývoj technologií, ale nás, uživatelů.

Ve Smart City se bude žít příjemně. Moje představa vychází ze zkušenosti, že jen to, co bude lidem příjemné, má budoucnost. A že budeme ochotni kvůli tomu změnit svoje zvyky. Klíčovým prvkem rozvoje chytrého města je podle mě chytrá doprava. Rychlý a bezpečný pohyb po městě je tím zásadním, co lidé dnes žádají. Cestování v současné podobě je nekomfortní, trvá dlouho a je vyčerpávající a tudíž nepříjemné. Pohyb po městě je činností, kterou nelze eliminovat. Stavebními kameny chytré dopravy pak bude především pokročilé inteligentní řízení dopravy, sdílení (informací i dopravních prostředků) a využití technologií neznečišťujících životní prostředí.

Co chceme? Více volného času? Déle spát? Nebo...?

Dalším významným prvkem chytrého města budou chytré domy, chytré byty a chytré domácnosti. Mám na mysli především inteligentní budovy, optimalizaci využívání energií (alternativní zdroje) a komfortní, plně customizované služby pro každého

Doprava v chytrých městech se musí stát rychlejší a příjemnější

Část práce za nás převezmou roboti

uživatele. Můžeme se bavit i o chytrém životním prostředí, o chytré ekonomice, případně o dalších oblastech. Základem Smart City z pohledu uživatele je nativní přístup. Pokud chci něco udělat, udělám to způsobem, který mě napadne jako první a bez dalšího obtěžování dosáhnu požadovaného efektu. Pokud bude takto fungovat koncept Smart City, budou lidé spokojeni a bude se jim žít příjemně.

Co bychom chtěli jinak? Více volného času? Déle spát? Nechodit do práce? Nepracovat? Více času na zábavu? Více možností zábavy?

Moderní město určitě zrychlí cestování. Dnes někteří lidé tráví cestou do práce a zpět mnoho času, a to se určitě postupně změní. Na druhé straně stále více lidí chce a pracuje z domova, tedy necestuje do práce vůbec. Počet pracovních pozic, který tento model práce umožní, bude s růstem informačních a zejména komunikačních technologií stále větší. Rutinní práce budou dělat roboti a tvůrčí práce se dá většinou dělat z domova. To bude klást zase větší nároky na inteligentní bydlení.

Doprava: Pomůže jen revoluční řešení

Ve vizích, spojených s chytrou dopravou, nemáme úplně jasno. Měla by být co nejefektivnější, tedy v co nejkratším čase přepravit co nejvíce cestujících, příjemně a bez obtěžování. Měla by tedy spojovat výhody hromadné a individuální dopravy. Hromadná doprava dokáže přepravit masu lidí, ale s čekáním, hlukem, s přestupy a dalšími nepříjemnostmi. Individuální automobilová doprava je pohodlná, auto jede, kdy chci a kam chci, ale musím ho pořád řídit, čekat v kolonách a zácpách. Navíc zabírá ve městě místo, kterého je stále méně. A to i tehdy, když nejede.

Inteligentní luxus nebude zadarmo

Oba typy přepravy se evolučně vylepšují. Mění se i přístup, auta lze sdílet a tím část nevýhod eliminovat, ale v určitém okamžiku dosáhnou svých hranic daných filosofií u každého typu cestování. Řešení musí být revoluční a bude určitě kombinací více přístupů. Klíčový opět bude komfort uživatele a jednoduchost. Pokud si hlasovým vstupem navolím cíl cesty, opustím svůj byt a jsem nejefektivnějším způsobem přepraven k cíli, tak to bude fungovat.

Chytré služby seberou část soukromí

S chytrou domácností je to maličko jednodušší. Tam už je ve vizích vidět za první horizonty. Dnešní pojetí chytrých domů je spojeno především s řízením na dálku a automatizovanými systémy ovládání čehokoliv. Od garážových vrat přes žaluzie na oknech až po topení, klimatizaci a dohledování domácnosti. Vyšším stupněm bude kontrola zásob v lednici a automatické doobjednání zásob v případě potřeby. A také automatické zajišťování vlastní údržby domu, inspirované současnými moderními automobily.

Pokud budeme chtít využívat inteligentní služby, budeme muset obětovat část svého soukromí. Jestliže chceme poslouchat svoji oblíbenou hudbu, jíst své oblíbené jídlo nebo mít ve vaně správnou teplotu vody, musíme tyto informace předat systému. Základem všech chytrých řešení je přece to, aby se nás už podruhé neptala na již zodpovězené otázky. *Klíčem je a bude elektronická identita v hmotné či nehmotné podobě.*

Každému, co jeho jest

Základem chytrého města bezpochyby bude plně customizovaný přístup. Každému, co jeho jest. Chytré bydlení, chytrá doprava i další prvky Smart City budou vyžadovat

bezpečnou a přívětivou identifikační metodu. Určitě se nebude jednat o jediné řešení, ale o celý technologický komplex.

Základem budou pravděpodobně technologie snímající podobu konkrétní osoby (rekognoskace obličejových rysů, detekce pohybu, rozpoznávání chůze). Tyto metody umožní naši identifikaci na dálku bez zvláštního zásahu a na poměrně vysoké úrovni bezpečnosti. Zejména kombinací různých metod lze úspěšně eliminovat chyby a dosáhnout vysoké přesnosti. Představme si například, že nás při příchodu domů snímá kamera, která ověří naši podobu a vzorec chůze. A pokud ještě následně naskenuje naše otisky při vstupu do dveří, systém se už nemusí na nic ptát a elektronický zámek nás vpustí domů.

Významnou roli budou hrát i bezkontaktní technologie, pravděpodobně propojené s mobilními komunikátory nebo nositelnou elektronikou. Jako příklad uvedu využívání integrovaných dopravních systémů či nákup lístků do divadla. S výhodou by se zde dala kombinovat identifikace osoby i s platební metodou.

Nejbezpečnější identifikace bude čipová

V budoucím Smart City bude nejvyšší formou bezpečné identifikace karta (token) s kontaktním čipem.

Bude sice užívána zřídka (což bude zvyšovat i její bezpečnost), ale bude spojována především s projevem vůle vlastníka. Závažná a závazná rozhodnutí, jako například nákup něčeho cenného, velké finanční operace nebo i aktivace či management identifikačních

Nejvyšší formou bezpečné identifikace je karta s kontaktním čipem

Bojíte se o svá osobní data? Tak proč o sobě na sociálních sítích prozrazujeme skoro vše...

nástrojů nižší bezpečnostní úrovně, bude spojen s použitím kontaktních technologií s vysokou mírou zabezpečení.

Elektronická identifikace bude ve valné většině případů nativní, nebude vyžadovat přímou součinnost identifikované osoby. V určitých případech, které si představme dnešním viděním tam, kde se musíme podepsat, bude potřeba projev vůle dané osoby.

I když předpokládáme, že svět papíru postupně bude ztrácet svoje postavení, úloha podpisu jakožto projevu vůle nezmizí. Jen se bude jednat o ***podpis elektronický***, který má podle mého názoru velkou budoucnost.

Komfort ve Smart City je dán mimo jiné i právem zvolit si, jak má vypadat a jak fungovat moje okolí, můj svět. Své preference ale musím být schopen systému sdělit, průběžně je měnit a upravovat a musí být zřejmé, že jde o mou vůli. Chování Smart City ke mně se změní, jen když k této změně dám souhlas, projevím vůli ke změně.

Na sociálních sítích vyzradíme (skoro) vše

Myslím si, že nejsprávnější cestou k nalezení kompromisu mezi systémem, který o nás ví vše, prakticky se na nic neptá a už umí vše zařídit (za což bychom zaplatili totální ztrátou soukromí), a systémem, který o nás neví nic a tudíž pro nás logicky nemůže nic udělat, je nechat na každém, ať si vše rozhodne sám.

Na jedné straně některá data úzkostlivě střežíme – například informace o zdravotním stavu, výši příjmu nebo sexuálních preferencích. Na straně druhé jsme schopni na sebe na sociálních sítích vyzradit i věci, které o nás neví ani nejbližší rodina. Vhodnou hranici mezi uživatelskou přívětivostí, důvěrou v systém a ochranou soukromí budeme hledat těžko a navíc se bude v čase vyvíjet.