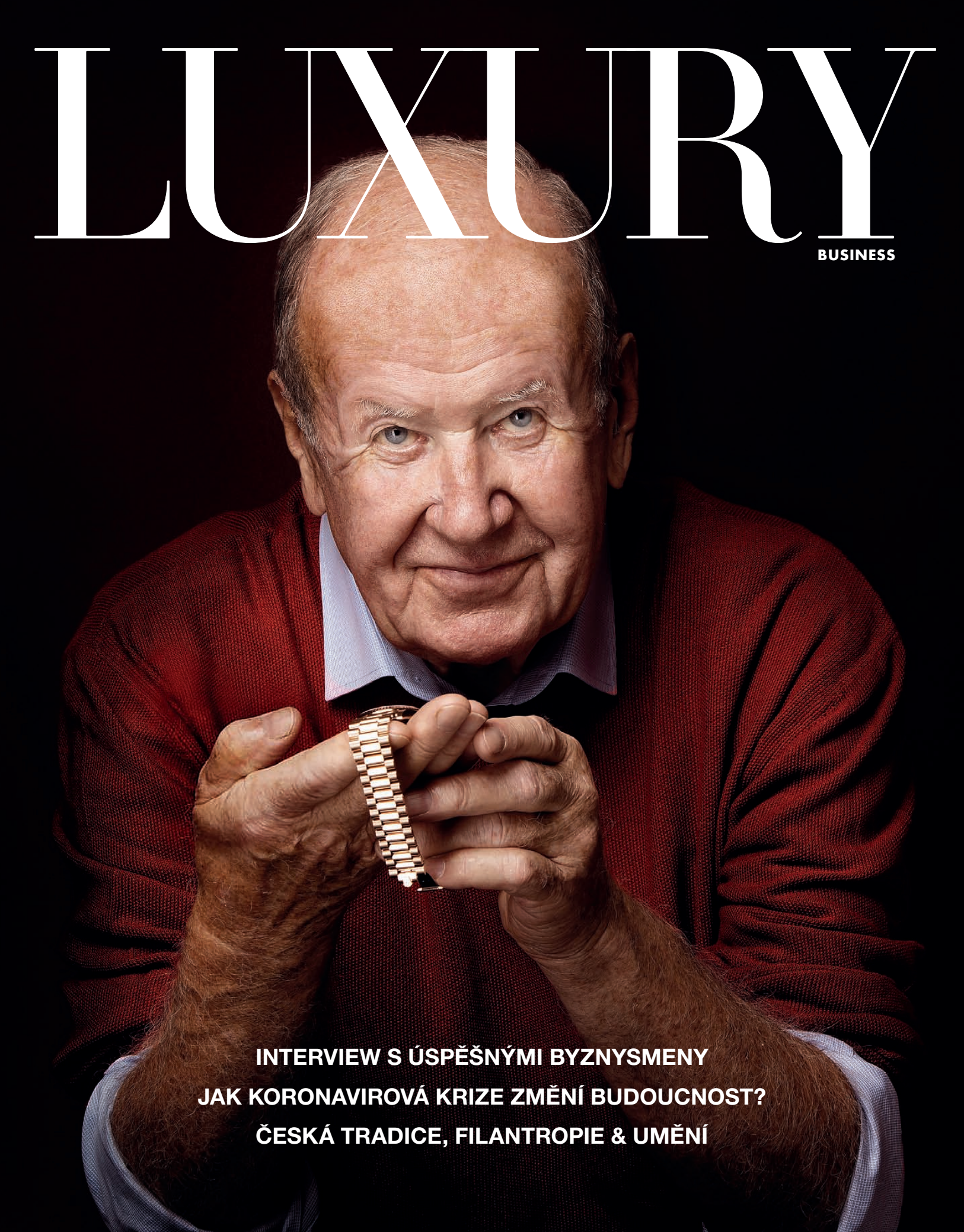
LUXURY

BUSINESS



INTERVIEW S ÚSPĚŠNÝMI BYZNYSMENY

JAK KORONAVIROVÁ KRIZE ZMĚNÍ BUDOUCNOST?

ČESKÁ TRADICE, FILANTROPIE & UMĚNÍ

Karol Suchánek: „Kybernetická bezpečnost bude rodinným stříbrem.“

V šestnácti letech vyvinul svůj první bezpečnostní software, absolvoval speciální cyber security program na MIT v Bostonu, je držitelem bezpečnostní prověrky NATO. Posledních deset let se stará o soukromí a bezpečnost firem a veřejně známých osobností po celém světě. Jeho cílem je dostat dovednost osobní digitální bezpečnosti mezi co nejvíce lidí.

připravil MICHAL VEČEŘA

Můžete mi jako laikovi stručně vysvětlit základní význam pojmu cyber security, neboli kybernetická bezpečnost?
Nejzákladnější vysvětlení je, že se jedná o zabezpečení jednotlivce nebo organizace proti hrozbám útoků vedených takzvanými hackery přes technologie připojené k internetu. Cílem takových útoků je narušení soukromí nebo zcizení informací.

Jak často se to děje?
Během posledních let se o různých únicích dat a nabourání soukromí dozvídáme z médií téměř denně. A jde o závratná čísla co do počtu lidí, jejichž data se tak dostávají do nepovolaných rukou. Třeba hackerský útok na americký registr dlužníků Equifax v roce 2017 se dotkl 147 milionů lidí, což bylo v té době 56 procent Američanů.

Mezi firmami jsou velké rozdíly v tom, s jakým objemem informací pracují. Platí, že čím menší množství dat firma spravuje, tím méně je útoky ohrožena?
To je jeden z hlavních mýtů. Nemusíte provozovat e-shop s miliony zákazníků, jejichž data evidujete, abyste byl pro hackery zajímavý. I pokud jste drobný živnostník a máte v počítači pouze data o svých zaměstnancích a dodavatelích, už se vás týká riziko útoků. V první linii probíhají automatizovaně a plošně. Hackeři používají softwarové roboty, které projíždějí internet a hledají bezpečnostní díry, jimiž se mohou do jednotlivých systémů dostat. Stejně automatizovaně jsou také rozesílané takzvané phishingové e-maily, které buď přímo obsahují škodlivý malware, nebo svým obsahem zmanipulují uživatele, aby se proklikl na nebezpečnou internetovou stránku nebo otevřel přílohu.

Co se děje dál?
Celá řada různých scénářů, které ale mají většinou jedno společné: dlouho o ničem nevíte. V tom se kybernetická kriminalita velmi liší od té fyzické. Když vám někdo přes noc ukradne auto, ráno o tom víte a můžete to začít řešit. U útoků na informační systémy ale není výjimkou, když jsou data bez povšimnutí kradena po dobu týdnů, měsíců, či dokonce let, podle sofistikovanosti celého postupu. Například hotelová síť Marriott zjistila v roce 2018, že jí někdo přes díru v IT infrastruktuře krade data o zákaznících už celé čtyři roky! Podle statistik většina firem odhalí hackerský útok až za tři měsíce. Hackeři pak získané informace buď prodávají dál, nebo přistoupí k vydírání. Může se jim podařit data na disku počítače zašifrovat a uživatel k nim nemá přístup. Za jejich rozšifrování pak požadují výkupné.

Takže když má firma data zálohovaná i jinde, má tento problém vyřešený?
Pokud odmítnete výkupné zaplatit, může dojít na výhrůžky, že data budou zveřejněna. To už může být velký problém vhledem k GDPR. Podle něj jste zodpovědný za ochránění veškerých informací o jednotlivcích i organizacích, které spravujete.

Je pak lepší výkupné zaplatit?
V tom nelze jednoznačně poradit. Jde v podstatě o jednání se zločinci – nikdy není záruka, že když zaplatíte výkupné, skutečně ještě neprodají data dál nebo je nezveřejní. Proto je jedinou dobrou cestou takovému problému předcházet, na což ale stále velká část firem nedbá, a to z různých důvodů. Často jde o přesvědčení, že nemají o co přijít, což už kvůli zmíněnému GDPR není pravda. Roli také hraje, že bezpečnost je samozřejmě náklad, který není v řadě firem populární. Když nalejete nějaké peníze do marketin-

„Třetí světová válka, která jednoznačně už v on-line světě probíhá, je bojem technologií a potažmo peněz. Kdo jich má víc, je napřed ve vývoji,“ tvrdí Karol Suchánek.

„Až 95 procent všech úniků informací z organizací je způsobeno lidským faktorem.“

gu, vidíte obchodní dopad. Utratíte-li za bezpečnost, na první pohled se nic nemění.

Není to způsobeno vysokou cenou?
Vtip je, že vysoká vůbec být nemusí, a především je vždy nesrovnatelně nižší, než jsou náklady na řešení vzniklých potíží – žehlení poškozené reputace a pokuty. Představte si firmu s globálním působením. Když dojde k úniku z české pobočky, zaplatí firma pokutu ve výši čtyř procent obratu, který má po celém světě. Při obratu třeba sto milionů se už jedná o celkem horentní sumu, jakou většinou zdaleka není nutné do prevence investovat. Firmy už spíš používají systémy, které nabízejí bezpečnostní funkce, jen je nemají dobře nastavené. Potřebují tedy především kvalitně provedený bezpečnostní audit.

Na kolik taková bezpečnostní revize firmu přijde?
Ceny se samozřejmě odvíjejí od velikosti organizace. Vždy však platí, že každý krok k lepšímu zabezpečení vytváří další pomyslnou ochrannou vrstvu – a čím více je těchto vrstev, tím méně je systém pro útočníky zajímavý. Je tedy vždy lepší udělat alespoň nějaké kroky a podle dostupného budgetu ochranu postupně vrstvit než nedělat nic. My v Shift2Cloud nabízíme základní audit bezpečnosti v ceně do dvaceti tisíc korun. Firma tak získá přehledný report se seznamem potřebných změn v nastavení systémů, které už může provést její vlastní IT specialista. Ruku v ruce s tím by mělo jít proškolení lidí. Až 95 procent všech úniků informací z organizací je způsobeno lidským faktorem. Buďto tím, že zaměstnanec naletí na phishingový e-mail, nebo sdělí nějaké informace v odpovědi na chytře zvolený dotaz.

Jak by tedy měli jednotlivci sami rozvíjet svoji bezpečnostní gramotnost?
Předně je třeba si uvědomit, že pokud vlastním počítač nebo mobil připojený k internetu, kybernetická bezpečnost se mě týká. Data, která jsou nějakým způsobem zneužitelná, nejsou zdaleka jen fotografie, čísla bankovních účtů nebo hesla. Lidé toho na sebe prozradí mnoho i na sociálních sítích. Třeba ze selfie fotografie je zřejmé, jakou máte značku telefonu... Musíme tedy hodně zvažovat, jaké informace o sobě zveřejníme, protože se mohou stát dílkem ve skládačce. Zároveň je důležité se vzdělávat v tom, jaké možnosti zabezpečení nabízí technologie, které používám. Brzy zjistíte, že celou řadu bezpečnostních opatření zvládnete sám. Třeba právě nastavení soukromí na sociálních sítích. Když přestanete svůj počítač používat v režimu administrátora, můžete se vyhnout některým počítačovým virům, které díky omezeným právům vašeho účtu nebudou mít možnost vykonávat škodlivé operace. Jde o změnu v nastavení uživatelského účtu vyžadující jen pár kliknutí. Sám chystám online kurz na www.securifit.com, který člověka jednotlivými kroky provede.

Poradíte nějakou šikovnou vychytávku?
Mnoho online služeb uchovává data o svých uživatelích, především e-mailové kontakty, i po zrušení účtu ve službě. Takovou stopu po sobě zanecháváme pokaždé, když se v nějaké službě zaregistrujeme, protože ji chceme vyzkoušet. I když nám pak nevyhovuje a účet zrušíme, nemáme jistotu, že také náš e-mail byl z databáze této služby odstraněn. Pro takové případy je skvělý nástroj www.10minutemail.com. Mailovka, kterou si zde založíte, za deset minut zanikne, takže ji můžete s klidem použít pro registraci ve službě, u níž si nejste jistí kvalitou. Když vám pak služba vyhovuje a rozhodnete se ji používat, prostě si založíte nový účet se svojí běžnou mailovou adresou.

Podílíte se na vzdělávání ve školách?
Ano. Baví mě kontakt s dětmi a snažím se jim téma kybernetické bezpečnosti zprostředkovat zábavně. Rozhodně je důležité, aby se základy dozvídaly od svých rodičů. Věřím, že jako se dřív z generace na generaci předávalo rodinné stříbro, bude se dědit i dovednost bezpečnosti v kyber prostoru.

Podle čeho vybírat odborníka na kybernetickou bezpečnost? Hlavním faktorem je podle Suchánka hodnocení zákazníků. Dále jde také o kvalitě vypovídají certifikace různých autorit, tedy bezpečnostní prověrky na úrovni států nebo mezinárodních organizací, jako je NATO. Ty jsou zárukou toho, že daný odborník není zatížený nějakými dluhy a úvěry, zná legislativu a je morálně bezúhonný.

FOTO: ARCHIV, WWW.KAROLSUCHANEK.COM