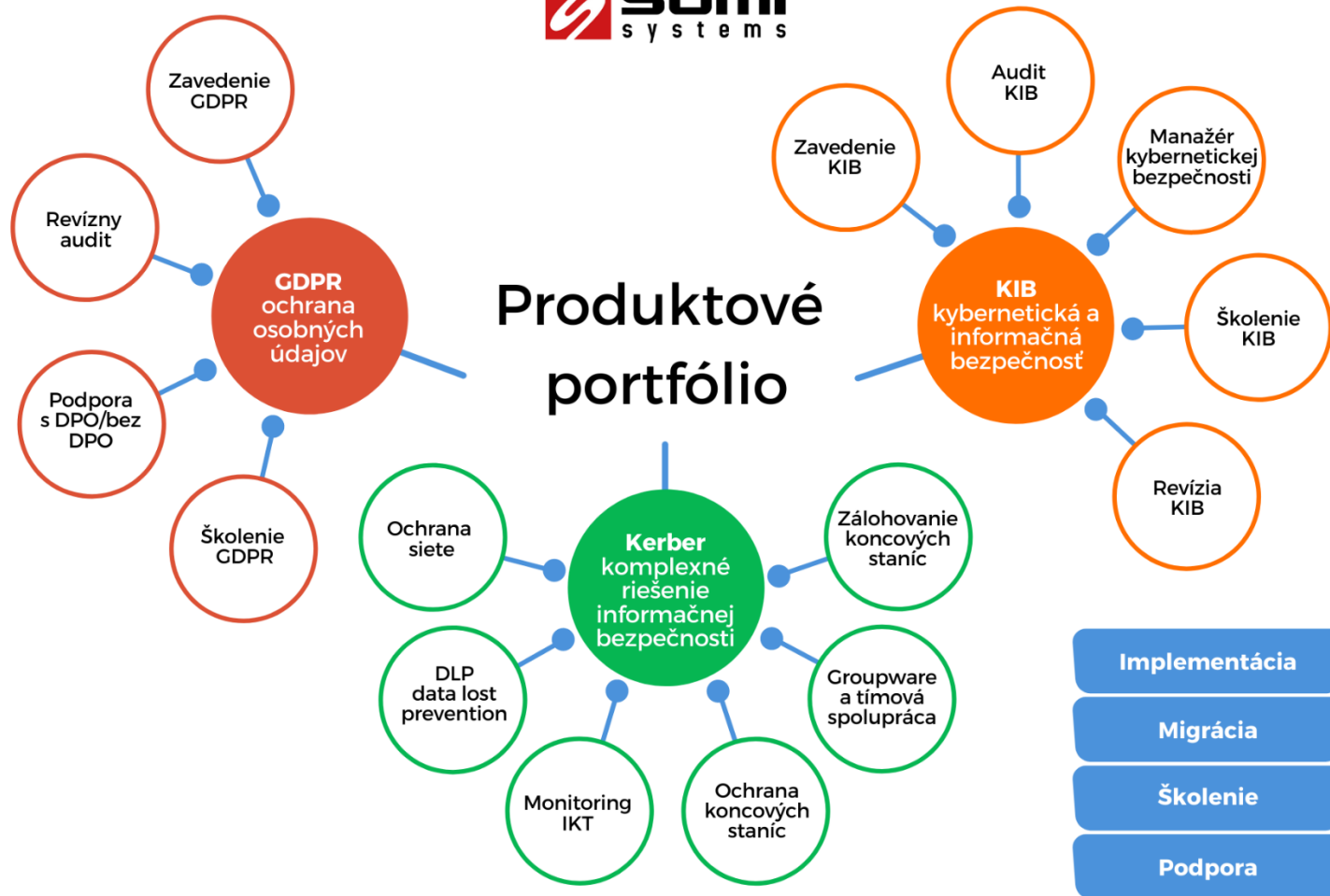




SOMI Systems a.s.

- ✓ úspešne zvládnutých **29 rokov** na poli informačnej a kybernetickej bezpečnosti, spolu s viac ako **400 spokojnými zákazníkmi**
- § riešime všetky Vaše otázky spojené s **kybernetickou bezpečnosťou, vrátane technických riešení**
- § sme profesionáli v implementácii nariadenia **GDPR** a výkonom funkcie **Zodpovednej osoby**
- OK 12 ročný vývoj **vlastnej produktovej rady** 
- 👍 **garancia nadštandardnej podpory a supportu**
-  **pravidelné školenia, e-learning a vzdelávania**

Viac informácií na www.somi.sk a www.kerber.sk



V SOMI Systems a.s. sme presvedčení, že nevyhnutnou súčasťou dnešnej rýchlo meniacej sa doby v technologickom svete je zdieľanie informácií.



Preto spolu s každou nami realizovanou službou, získavate aj prístup k plnohodnotným školeniam, pravidelnému vzdelávaniu, eLearningom, najnovším článkom na blogu a vzdelávacím infografikám.

Pár infografík Vám prinášame na ukážku.

Viac informácií na www.somi.sk a www.kerber.sk



KYBERNETICKÉ HROZBY PRE ROK 2022

NA ČO KONKRÉTNE SI DÁVAŤ NAJVVÄČŠÍ POZOR
V ROKU 2022 NA SLOVENSKU

Zdroj: Kaspersky Security Bulletin, ESET, infosecurity.sk



SOFISTIKOVANÉ ÚTOKY NA MOBILNÉ ZARIADENIA

Smartfóny boli vždy pre útočníkov silným lákadlom, nakoľko cestujú so svojimi majiteľmi všade a sú úložiskom obrovského množstva cenných informácií.

STÁLE VIAC ÚTOKOV NA DODÁVATEĽSKÝ REŤAZEC

Takéto útoky sú pre útočníkov mimoriadne cenné, pretože umožňujú prístup k veľkému počtu potencionalných cieľov.

ÚTOKY ZAMERANÉ NA PRÁCU Z DOMU

Stále častejšie sa zneužívajú nechránené a neaktualizované domáce počítače. Sociálne inžinierstvo zamerané na krádež prihlasovacích údajov, šírenie ransomwaru a útoky hrubou silou na podnikové služby s cieľom získať prístup k slabo chráneným serverom budú pokračovať.

VÝZNAMNÝ NÁRAST ÚTOKOV NA ZABEZPEČENIE CLOUDU

Mnohé organizácie využívajúce cloud a tak isto ich poskytovatelia sa môžu stať zraniteľnejšími voči chybám, útokom alebo výpadkom. Hlavné dodávateľia cloudových služieb budú cieľom sofistikovaných útokov.

AŽ PRÍLIŠ INTELIGENTNÁ DOMÁCNOSŤ

Tým, že sú naše domácnosti stále viac prepojené, príležitosti útočníkov ako zasahovať do našich životov sa zvyšujú. Smart TV, robotický vysávač, domáca IP kamera, video vrátnik sú prepojené cez IoT a domácu WiFi sieť. Inteligentné zariadenia majú často slabé stránky v oblasti bezpečnosti už od výroby.

ZNEUŽÍVANIE ZRANITELNOSTI APACHE KNIŽNICE Log4j

Hlavnými cieľmi týchto útokov budú aj naďalej používateľské heslá a prístupové údaje k bankovým službám. Najčastejším cieľom týchto útokov sú tie najpoužívanejšie služby a softvér - Windows, macOS, MA Exchange, Azure AD, Chrome, Edge a Firefox.

PODVODY ZNEUŽÍVAJÚCE AKTUÁLNE TÉMY

Napríklad Olympijské hry a Majstrovstvá sveta vo futbale sa budú zneužívať k ponukám falošných vstupeniek, plateným nelegálnym streamom, podvodným marketingovým ponukám a šíreniu vírusových infiltrácií. Nové podvody a útoky sa očakávajú aj v oblasti kryptomén a NFT - cryptojacking a útoky na peňaženky.

Viac zaujímavých informácií nájdete aj na našom blogu na
www.somi.sk



ZÁKLADNÉ ONLINE BEZPEČNOSTNÉ TIPY

AKTÍVNE SI CHRÁŇTE SVOJU
INTERNETOVÚ IDENTITU NA SOCIÁLNYCH
SIETACH



POUŽÍVAJTE SILNÉ HESLÁ

Používajte silné (malé a veľké písmená, číslice a špeciálne znaky), dlhé (kľudne aj 30 znakov) heslá, ktoré je ťažké uhádnuť a pravidelne ich meňte (aspoň 2x do roka).
Např.: KEDprídemranodopravevpíjem1kavu!



DÁVAJTE POZOR NA ČO KLIKÁTE

Nie všetko, čo na obrazovke uvidíte je aj zákonite pravda - existuje mnoho internetových hrozieb (např. sociálne viry), ktoré zneužijú fotku a meno Vašeho priateľa a v jeho mene šíria nebezpečný obsah.

Tip: Nebuďte veselým klikárom, vždy a všetko si pozorne prečítajte pred tým, ako na to kliknete a pokiaľ niečo vyzerá až priveľmi zaujímavé a lákavé, je to pravdepodobne podvod - nikto Vám nedá nič zadarmo.



NASTAVTE SI SÚKROMIE

V nastaveniach sociálnych sietí si vie každý používateľ nastaviť a obmedziť viditeľnosť svojich osobných údajov. V štandardnom režime (po registrácii) sú Vaše osobné údaje a aktivity viditeľné pre kohokoľvek.

Upozornenie: súkromie nastavte aj svojim deťom.



MYSLITE PRED TÝM AKO NIEČO ZVEREJNÍTE

Vyhňte sa zverejňovaniu citlivých osobných údajov a nezdieľajte príliš veľa informácií.

Tip: nezabúdajte, že všetko čo na internete zverejníte, zostane tam navždy.



VŽDY POUŽÍVAJTE ANTIVÍRUS

Každé zariadenie, ktoré sa pripája do internetu, by malo mať pravidelne aktualizovaný antivírusový program.

Tip: nezabúdajte na Vaše smartfóny, aj na nich majte nainštalovaný aspoň free antivírus.

Viac zaujímavých informácií nájdete aj na našom blogu na
www.somi.sk



EFEKTÍVNY SPRIEVODCA AKO MAŤ

E-MAILOVÚ SCHRÁNKU BEZ SPAMU



V roku 2020 sa denne odoslalo 306 400 000 e-mailov a 50,37% zo všetkých týchto e-mailov tvoril spam a Slovensko nie je výnimkou.

13% používateľov na Slovensku v roku 2021 aspoň raz otvorilo prílohu z phishingového e-mailu.



Väčšina útokov je finančného charakteru:

- podvodné eshopy a strata peňazí
- strata údajov z platobnej karty
- sprístupnenie internet bankingu
- podvody pri mobil bankingu

9 ZÁSAD

AKO UDRŽAŤ E-MAIL SCHRÁNKU



BEZ SPAMU

A PHISHINGOVÝCH E-MAILOV

- 1 ODPAD PATRÍ NA SMETISKO**
Odstráňte nevyžiadané e-maily pred ich otvorením a zakážete automatické sťahovanie obrázkov.
- 2 POUŽÍVAJTE VSTAVANÉ SPAM FILTRE**
Sú súčasťou najpopulárnejších e-mailových služieb.
- 3 VYBERTE SI ZLOŽITÚ ALEBO NEZVÝČAJNÚ E-MAILOVÚ ADRESU**
Spameri používajú sofistikované roboty generujúce mená, ktoré chýlia miliardy možných kombinácií e-mailových adries.
- 4 BUĎTE OPATRNÝ PRI ZAPISOVANÍ VAŠEJ E-MAILOVEJ ADRESY**
Nezverejňujte svoju e-mailovú adresu na webových stránkach alebo na profiloch sociálnych médií.
- 5 POUŽÍVAJTE JEDNORÁZOVÉ E-MAILOVÉ ADRESY**
Využite túto možnosť, keď potrebujete e-mailovú adresu na odoslanie správy do fóra alebo na pripojenie sa ku skupine. Existuje veľa bezplatných služieb e-mailových adries.
- 6 POUŽÍVAJTE ANTISPAMOVÉ A ANTIVÍRUSOVÉ PROGRAMY**
Snažte sa ich mať vždy aktualizované a všimajte si čo s Vami komunikujú.
- 7 UČTE SPAM FILTER VO VAŠOM E-MAIL KLIENTOVI**
Ručne označte všetky nevyžiadané e-maily ako spam, keď prejdú Vaším spam filtrom.
- 8 ODHLÁSTE SA ZO ZOZNAMOV ADRIES (UNSUBSCRIBE)**
Zbavte sa ťžitov času a poutrajte si vo Vašej doručenej pošte. V skutočnosti Vám nemusí denne prichádzať 20 reklamných e-mailov aby Vám náhodou neušla nejaká akciová ponuka.
- 9 NIKDY NIČ V SPAMOCCH NEPOTVRDZUJTE**
Každá Vaša odpoveď potvrdzuje, že Váš e-mail je skutočný a platný.

Viac zaujímavých informácií nájdete aj na našom blogu na www.somi.sk



ZÁKLADNÉ PHISHINGOVÉ ÚTOKY

PHISHING STÁLE PREDSTAVUJE JEDNU Z NAJPOUŽÍVANEJŠÍCH METÓD PRE KRÁDEŽ VAŠICH PRÍSTUPOV A PEŇAZÍ.



AK VÁM PRÍDE EMAIL (S PRÍLOHOU ALEBO LINKOM) O KTORÉHO BEZPEČNOSTI SI NIE STE ISTÝ, POSTUPUJTE PODĽA NIŽŠIE POPÍSANÝCH SCENÁROV.



OVERENIE ÚČTU

- Príde Vám email, ktorý na prvý pohľad vyzerá, že pochádza od známej spoločnosti (Netflix, Youtube, ...) a žiada Vás, aby ste sa prihlásili a opravili problém s Vaším účtom, prípadne reagovali na nejakú ponuku alebo zmenu.
- Odkaz odkazuje na webovú stránku, ktorá predstiera, že je legitímnou stránkou danej spoločnosti a vyžaduje Vaše prihlasovacie údaje.

TIP: VŽDY PRED KLIKOM NA ODKAZ, SI NAJPRV PREKONTROLUJTE KAM SKUTOČNE SMERUJE

BANKOVÝ PHISHING

- Príde Vám email, ktorý na prvý pohľad vyzerá, že pochádza od Vašej banky a žiada Vás, aby ste sa prihlásili do internet bankingu, reagovali na nejakú výhodnú ponuku úveru, poprípade overili svoju platobnú kartu.
- Odkaz odkazuje na webovú stránku, ktorá predstiera, že je legitímnou stránkou banky a vyžaduje Vaše prihlasovacie údaje.

TIP: VŽDY BUĎTE RADŠEJ SKEPTICKÝ POKIAĽ SA JEDNÁ O AKTÍVA PRE VÁS CITLIVÉ. KEĎ SA VÁM NIEČO NEPOZDÁVA, RADŠEJ KONTAKTUJTE SVOJU BANKU

ZDIEĽANIE CEZ CLOUD

- Príde Vám email, ktorý obsahuje odkaz na niečo, čo sa javí ako zdieľaný súbor v cloud službe (SharePoint, One Drive, Dokumenty Google, Evernote, ...) alebo inej lokalite na zdieľanie súborov.
- Odkaz odkazuje na webovú stránku, ktorá predstiera, že ide o lokalitu na zdieľanie súborov, a vyžaduje, aby ste sa prihlásili.

TIP: NIKDY NEOTVÁRAJTE PRÍLOHY V EMAILOCH OD ODOŠIELATEĽOV KTORÝCH NEPOZNÁTE

FALOŠNÉ FAKTÚRY A VÝZVY NA ÚHRADU

- Príde Vám email, ktorý obsahuje doklad prezentovaný ako neuhradená faktúra (výzva na úhradu, exekučný príkaz).
- Útočníci cieľia na jednotlivcov (napr. predstieraním, že sú exekútori) alebo organizácie (vydávaním sa za predajcu alebo dodávateľa) s úmyslom sa obohatiť na úkor obete.

TIP: VŽDY SI PREKONTROLUJTE ADRESU ODOŠIELATEĽA EMAILU

FALOŠNÉ OZNÁMENIA O DORUČENÍ

- Príde Vám email, ktorý obsahuje informáciu o možnosti doručenia zásielky, ale treba doplatiť poplatok za doručenie.
- Útočníci sa schovávajú za známe spoločnosti u nás - Slovenská pošta, SPS, DHL ...

TIP: VŽDY VŠETKO POZORNE ČÍTAJTE, KLUDNE A JAK VIAC KRÁT



Viac zaujímavých informácií nájdete aj na našom blogu na www.somi.sk



10 TIPOV PRE BEZPEČNÉ HESLO

AKO NA POLITIKU HESIEL BEZPEČNE A JEDNODUCHO



Najpoužívanejšími heslami na Slovensku v roku 2021 boli napríklad aj:

- 123456, ktoré bolo použité 111 800x a prelomené je za menej ako 1 sekundu
- qwerty, ktoré bolo použité 27 490x a prelomené je za menej ako 1 sekundu
- martin, ktoré bolo použité 9 332x a prelomené je za menej ako 2 minúty
- heslo, ktoré bolo použité 7 513x a prelomené je za menej ako 10 sekúnd
- monika, ktoré bolo použité 7 282x a prelomené je za menej ako 1 sekundu
- milacik, ktoré bolo použité 5 200x a prelomené je za menej ako 17 minút

Zdroj: <https://nordpass.com/most-common-passwords-list/>

- DODRŽIAVAJTE PRIJATÚ POLITIKU HESIEL**
Pokiaľ má Vaša organizácia zavedené vlastné zásady pre bezpečnosť hesiel, vždy ich dodržiavajte v tej najbezpečnejšej forme (16 znakov v hesle je viac ako 8 znakov).
- DLHŠIE HESLO JE VŽDY BEZPEČNEJŠIE**
Používajte heslá, ktoré majú malé a veľké písmená, číslíce a špeciálne znaky, ale hlavne majú aspoň 12 znakov. Každým pridaným znakom zvyšujete bezpečnosť hesla.
- POUŽÍVAJTE FRÁZY A NIE SLOVÁ**
Kľudne použite frázu, ktorá má aj 20 znakov. Keď je pre Vás ľahko zapamätateľná a priradíte k nej veľké písmo a číslo, získate bezpečné heslo. Napr.: KEDpridemranodopravevprijem1kavu
- NEPOUŽÍVAJTE BEŽNE POUŽÍVANÉ SLOVÁ**
Nikdy v heslách nepoužívajte bežné slovníkové slová a ani nič čo je o Vás verejne známe (pripadne ľahko uhádnuteľné (napr. mená a dátumy rodinných príslušníkov)).
- POUŽÍVAJTE TO, ČO POZNÁTE LEN VY**
Čokoľvek čo obsahuje dostatočný počet znakov, malé a veľké písmená, číslíce a znaky a zmysel to dáva len Vám, je bezpečné heslo. Tip: používajte dlhé frázy
- HESLO SI NIKAM NEZAPISUJTE**
Vytvárajte si heslá, ktoré si zapamätáte bez toho, aby ste si ich museli kdekoľvek zapisovať. Ak nie, zapíšte si len nápovedu ktorá bude dávať zmysel len Vám.
- NEPOUŽÍVAJTE BEŽNÉ ZÁMENY ZNAKOV**
Je bežnou praxou, že sa v heslách nahrádza slovo alebo číslíca za znak (o za 0, e za 3). Pre útočníkov je toto známy fakt a určite si týmto spôsobom neposilníte Vaše heslo.
- S HESLAMI SA NEOPAKUJTE**
Pre každý účet používajte jedinečné heslá - nikdy jedno heslo nepoužívajte pre viacero prístupov. Nepoužívajte heslá, ktoré ste už v minulosti použili.
- AK TO NEFUNGOVALO V MINULOSTI, NEBUDE TO FUNGOVAŤ ANI TERAZ**
Tie najjednoduchšie a najbežnejšie heslá sú a vždy budú závažným bezpečnostným rizikom, nakoľko ich dešifrovanie (uhádnuť) je rádovo v sekundách bežnými nástrojmi.
- HESLO S NIKÝM NEZDIEĽAJTE**
Heslo je ako zubná kefka - pravidelne si ju meníte a určite ju s nikým nezdieľate.

Viac zaujímavých informácií nájdete aj na našom blogu na www.somi.sk



HESLÁ, HESLÁ, HESLÁ

AKÉ HESLÁ NIKDY NEPOUŽÍVAŤ A ČO JE VHDNÉ POUŽÍVAŤ PRI HESLÁCH



Illustration showing bad password examples (123456, qwerty, martin, monika, laska, heslo, 1qay2wsx, milacik, futbol, 1q2w3e) and good password examples (vzdypouzivajteakohezlonejakufrazu, CIMdlhsieheslopouzijetetyjmjebezpecnejsie!, DOVolenka2022...). A large red 'X' is placed over the bad examples, and a green checkmark is placed over the good examples. A laptop screen shows 'martin' and a USB drive is shown.

Viac zaujímavých informácií nájdete aj na našom blogu na www.somi.sk



10 TIPOV PRE FYZICKÚ BEZPEČNOSŤ

OCHRANA DOKUMENTOV A PRACOVISKA AKO NEVYHNUTNÁ SÚČASŤ BEZPEČNOSTI

Ekonómická a majetková kriminalita na Slovensku v roku 2020:

- 325 lúpeží
- 11 216 ekonomických trestných činov
- ekonomickou kriminalitou bola spôsobená škoda viac ako 235 miliónov €
- 1 665 prípadov podvodu
- 18 715 majetkových trestných činov
- 3 725 krádeží vlámaním



Zdroj: Ministerstvo vnútra Slovenskej republiky

1 DODRŽIAVAJTE PRIJATÚ BEZPEČNOSTNÚ POLITIKU
Pokiaľ má Vaša organizácia zavedené vlastné zásady pre fyzickú bezpečnosť, vždy ich dodržiavajte v tej najvyššej možnej forme (smernice, interné pokyny).

2 PRACOVISKO
Každý zamestnanec je zodpovedný za fyzickú bezpečnosť svojho pracoviska - pri odchode treba vypnúť počítače, uzamknúť pracovisko a zavrieť okná.

3 ZVERENÉ PRACOVNÉ PROSTRIEDKY
Každý zamestnanec je zodpovedný za fyzickú bezpečnosť zverených pracovných prostriedkov - treba byť obozretný hlavne pri zariadeniach, ktoré opúšťajú kancelárie.

4 POČÍTAČE Tip: používajte klávesovú skratku win + L
Počítače udržiavajte vždy aktuálne, reagujte na správy z antivirusového programu a kolegov z IT a keď odchádzate od počítača, odhláste sa.

5 SPRÁVNE NATOČENÉ MONITORY Tip: používajte bezpečnostné fólie na monitor
Natočte si monitory tak, aby nebolo vidieť, čo práve robíte pre kohokoľvek cudzieho - dôležité hlavne v prípade, že ku Vám chodia návštevy.

6 PRAVIDLO ČISTÉHO PRACOVNÉHO STOLA
Zabezpečte, aby sa Váš pracovný stól nestal malým archívom spisovnej agendy. Pokiaľ odchádzate z pracoviska, snažte sa spisovú agendu uzamykať.

7 HESLÁ, HESLÁ, HESLÁ
Nikdy si heslá, používate ako vstup do operačných a informačných systémov nezapisujte na papieriky, kalendáre, nástenky, pod klávesnice atď.

8 DOKUMENTY V PAPIEROVEJ FORME
Vždy dohľadajte na to, že papierové dokumenty s osobnými alebo citlivými údajmi sú dostatočne chránené - pod Vašim dohľadom a v neprítomnosti uzamknuté.

9 KLÚČOVÝ REŽIM
Prípadnú stratu kľúčov ste povinný ihneď oznámiť kolegovi, ktorý zodpovedá za ich evidenciu.

10 SOCIÁLNE INŽINIERSTVO
Buďte obozretný v prípade neautorizovaných a podozrivých osôb pohybujúcich sa vo Vašich priestoroch - podvody tohto druhu sú aktívne zneužívané hlavne vo väčších organizáciách.

Viac zaujímavých informácií nájdete aj na našom blogu na www.somi.sk



JEDNODUCHÝ SPRIEVODCA AKO OCHRÁNIŤ OSOBNÉ A CITLIVÉ ÚDAJE



GDPR už nie je „len“ o nevyhnutnej legislatíve a s ňou spojenej agende, ale je to sústava procesov, ktoré sa raz vybudujú a budú sa neustále udržiavať a vylepšovať.

V roku 2020 Úrad na ochranu osobných údajov udeľoval pokuty za porušenie ochrany osobných údajov v rozmedzí 700 - 20 000 eur

V ROKU 2021 SA PRIEMERNÁ CENA UDELENÝCH POKÚT U NÁS ZVÝŠILA O 300%

KEĎ SA DODRŽIAVAJÚ SPRÁVNE NASTAVENÉ PRAVIDLÁ, KONTROLA NIE JE PROBLÉM.

9 ZÁSAD

AKO SA SPRÁVAŤ K OSOBNÝM ÚDAJOM



TAK, ABY STE O NE NEPRIŠLI

1 OSOBNÉ ÚDAJE ZBIERAJTE A POSKYTUJTE LEN V NEVYHNUTNOM ROZSAHU.

2 AK KOPÍRUJETE DOKUMENTY S OSOBNÝMI ÚDAJMI, SKARTUJTE ICH HNEĎ PO ICH SPRACOVANÍ.

3 DODRŽIAVAJTE PRAVIDLO ČISTÉHO STOLA A ZAMKNUTEJ OBRAZOVKY.

4 NEKLIKAJTE NA NEOVERENÉ A PODOZRIVÉ ODKAZY. NESPRÁVAJTE SA AKO VESELÝ KLIKÁR A VŽDY SI PREČÍTAJTE NA ČO CHCETE KLIKNÚŤ.

5 POUŽÍVAJTE SILNÉ HESLÁ A CHRÁŇTE ICH PRED ZNEUŽITÍM.

6 PRI POSIELANÍ SÚBOROV S OSOBNÝMI ÚDAJMI E-MAILOM, ŠIFRUJTE TIETO ÚDAJE NAPRÍKLAD POMOCOU ZIP, RAR PROTOKOLU.

7 NAHLÁSTE KAŽDÝ BEZPEČNOSTNÝ INCIDENT KOMPETENTNÝM HNEĎ AKO ZISTÍTE, ŽE NASTAL.

8 NA INTERNETE VÁM NIKTO NEDÁ NIČ ZADARMO - AK ÁNO, TAK BUĎ STE UŽ O NIEČO PRIŠLI, PRÁVE PRICHÁDZATE ALEBO ĎALŠÍM KLIKOM PRÍDETE.

9 PRAVIDELNE SA VZDELÁVAJTE V PROBLEMATIKE INFORMAČNEJ BEZPEČNOSTI A NEIGNORUJTE UPOZORNENIA, KTORÉ K VÁM SMERUJÚ.

Viac zaujímavých informácií nájdete aj na našom blogu na www.somi.sk

