SPRÁVNÉ REAKCE K ZAJIŠTĚNÍ KYBERNETICKÉ BEZPEČNOSTI

SAINT-GOBAIN

Každý den sehráváte klíčovou roli v zabezpečení firemních IT prostředků: když procházíte internet, používáte elektronickou poštu, otevíráte přílohy, zadáváte hesla, vypínáte váš počítač, stahujete software, používáte flash paměti, reagujete na případná upozornění na riziko kybernetického útoku atd.…

Abychom vám pomohli, zde jsou některé základní návyky a reakce, které je třeba v souvislosti s ochranou proti kybernetickým útokům dodržovat.

E-maily od externích subjektů

1 **Nikdy neotvírejte přílohy k e-mailovým zprávám, které jste obdrželi od neznámého odesílatele.**

nebo přílohy, jejichž název či formát ničím nepřipomíná obvyklý druh souborů, které od příslušného kontaktu dostáváte. Všechny typy souborů (Word, PDF, Excel atd.) mohou obsahovat virus.

2 **Je-li v e-mailové zprávě od neznámého odesílatele uvedena webová adresa, neklikejte na ni.**

Najedete-li kurzorem myši na uvedený link (aniž byste na něj kliknuli), zobrazí se vám skutečná adresa stránky, kam vás link po případném kliknutí přesměruje.

3 **Nikdy nereagujte na žádosti o důvěrné informace prostřednictvím elektronické pošty.**

(osobní údaje, důvěrné kódy např. pro obnovení přístupu k některým službám, čísla kreditních karet atd.)

4 **Máte-li pochybnosti o konkrétní e-mailové zprávě, kterou jste obdrželi do vaší schránky, přepošlete ji okamžitě na tuto adresu:** suspicious@saint-gobain.com

Osobní počítače

5 **Zvolte si bezpečné heslo a nikam si jej nezapisujte.**

Zvolte si opravdu bezpečné heslo (min. 12 znaků, je-li to možné: kombinace malých písmen, velkých písmen a speciálních znaků, např. & } + @, nebo slova, která nelze najít ve slovníku atd.). Silné heslo je takové, které třetí strany jen těžko prolomí hádáním nebo vygenerováním pomocí automatických nástrojů.

Nepoužívejte stejné heslo všude. Pro váš přístup do firemních aplikací, osobní pošty, k bankovním účtům atd. byste vždy měli používat jiná hesla.

6 **Každý večer vypínejte váš počítač.**

Do vašeho pracovního počítače se pravidelně stahují různé bezpečnostní aktualizace, které k nainstalování vyžadují restart vašeho počítače. Pokud se bezpečnostní aktualizace instalují ručně, udělejte to vždy bez otálení.

7 **Pokud jste vypli váš pracovní počítač a odpojili se od sítě Saint-Gobain na dobu delší než 1 měsíc, obraťte se před opětovným připojením na vaše oddělení podpory IT,**

aby pracovníci z tohoto oddělení mohli provést instalaci všech nezbytných bezpečnostních aktualizací.

8 **Jste-li často pryč ze své kanceláře, např. na služebních cestách, vždy připojte svůj pracovní počítač do sítě ve vašem závodě Saint-Gobain pomocí síťového kabelu alespoň jednou v průběhu prvních dvou týdnů v každém měsíci a poté ještě jednou ve zbývajících 2 týdnech ve stejném měsíci.**

Velikost aktualizací od společnosti Microsoft vyžaduje připojení do sítě v závodě Saint-Gobain pomocí síťového kabelu.

9 **Nepoužívejte vybavení / zařízení, jehož původ neznáte (například flash paměti nebo jiná přenosná paměťová média).**

Prostřednictvím nich se do vašeho pracovního počítače mohou dostat škodlivé programy či viry.

10 **Nestahujte do svého počítače žádný software, který není oficiálně povolený společností Saint-Gobain.**

Prostřednictvím něj se do vašeho pracovního počítače také mohou dostat škodlivé programy či viry.

11 **Svůj pracovní počítač nikomu nepůjčujte.**

Vybavení, které jste od společnosti dostali, musí sloužit jen k pracovním účelům a nesmíte jej proto půjčovat nikomu ze své rodiny ani cizím osobám. Také svá hesla nesmíte nikomu sdělovat.

12 **Jste-li na služební cestě, mějte svůj pracovní počítač neustále s sebou a nenechávejte ho bez dohledu na veřejných místech nebo ve vašem hotelovém pokoji.**

13 **Bude-li váš pracovní počítač odcizen nebo jej ztratíte, ihned kontaktujte vaše oddělení podpory IT.**

Chytré telefony a tablety

14 **Instalujte do svých zařízení pouze aplikace z Apple store nebo Play store. Navíc instalujte jen takové aplikace, které nezbytně nutně potřebujete k pracovním účelům.**

Některé aplikace mohou obsahovat škodlivé programy nebo viry, konkrétně aplikace určené pro chytré telefony s operačním systémem Android.

15 Vždy si zkontrolujte, k jakým údajům získají nainstalované aplikace přístup (lokalizace, kontakty, soubory...) a autorizujte pouze oprávněné přístupy.

E-maily a seznamy obchodních kontaktů ve vašem chytrém telefonu představují citlivé informace. Za citlivé informace se považují také důvěrné dokumenty, které mohou být v těchto e-mailech obsaženy.

16 Bude-li váš chytrý telefon či iPad odcizen nebo jej ztratíte, ihned kontaktujte vaše oddělení podpory IT.

Prohlížení internetu

17 Nevstupujte do prostředí internetu jinými způsoby, než prostřednictvím sítě Saint-Gobain.

Jste-li mimo společnost (například na vlakovém nádraží, na letišti, v hotelu, doma atd.) a připojíte-li se k internetu prostřednictvím veřejné Wi-Fi, okamžitě aktivujte vzdálené VPN připojení do sítě Saint-Gobain. Jedině tak bude váš přístup do internetu zabezpečený.

18 Nikdy neotvírejte přílohy z vašich osobních e-mailových zpráv (Gmail...) v pracovním počítači.

Přihlašujete-li se ke své soukromé poštovní schránce prostřednictvím vašeho firemního počítače, počínejte si velmi opatrně. Nikdy například neotvírejte přílohy ve vašich osobních e-mailových zprávách, neboť soukromé e-maily nejsou kontrolovány antivirovými programy Saint-Gobain a představují tak vysoké riziko infekce.

19 Neukládejte firemní data na vašich soukromých cloudech.

Na veřejných cloudových službách k ukládání dat (např. Dropbox atd.) není možné zaručit požadovanou bezpečnost.

20 Neukládejte firemní informace do vašich soukromých počítačů nebo chytrých telefonů.

Stane-li se váš soukromý počítač cílem hackerů, bude veškerá odpovědnost za únik firemních údajů a informací pouze na vás.

21 Nezveřejňujte firemní informace na sociálních sítích.

Informace, které publikujete na sociálních sítích, mohou být zneužity například ke zjištění vašich hesel, k přístupu do vašich IT systémů nebo dokonce ke krádeži vaší identity nebo průmyslové špionáži.

Kybernetický útok

22 Objeví-li se na vašem pracovním počítači obrazovka požadující výkupné, odpojte z počítače síťový kabel nebo se ihned odpojte od Wi-Fi.

Poté informujte pracovníky vašeho oddělení podpory IT a varujte i vaše kolegy.

23 Budete-li upozorněni pracovníky z oddělení podpory IT nebo vašimi kolegy na kybernetický útok, ihned odpojte síťový kabel z vašeho počítače nebo se odpojte od Wi-Fi.

Vypnutí počítače je pomalejší operace, než odpojení síťového kabelu. Navíc škodlivé programy a viry se mohou aktivovat právě po restartování vašeho počítače.

Budete-li mít i sebemenší pochybnost o zabezpečení vašeho vybavení, kontaktujte vaše oddělení podpory IT!