DESATERO OBRANY PROTI HACKU

1. **AKTUALIZUJTE – VŽDY A VŠECHNO** – aktualizace nejen systémů, ale i aplikací nebo firmware zařízení je nezbytným základem.

2. **ZÁLOHUJTE – VŽDY, VŠECHNO, NĚKOLIKRÁT a HLAVNĚ ZÁLOHY TESTUJTE –** zálohovat, zálohovat, zálohovat a ještě jednou zálohovat … ano přesně tak. Bohužel většina uživatelů začne zálohovat až po první ztrátě dat. Důležitý je samozřejmě monitoring záloh a jejich testování. Zároveň by všichni měli pamatovat na pravidlo 3_2_1, tedy mít tři zálohy na dvou různých systémech, přičemž jedna z nich by se měla nacházet v jiné geografické lokalitě.

3. **POZOR NA MAILOVÉ PŘÍLOHY – HLAVNĚ OD PŘÁTEL** - V srpnu 2019 bylo globálně odesláno přes 416 miliard nevyžádaných e-mailů a spam tak tvořil více než 85 procent všech odeslaných e-mailů. Podle studie Cisco Annual Cybersecurity Report přitom průměrně každý osmý až desátý z nich obsahuje infikovanou přílohu. E-mail je také nejčastějším nástrojem, který hackeři využívají pro napadení firem. Pozor taktéž na maily s upozorněním na neuhrazené faktury … stačí chvilka nepozornosti a peníze jsou fuč tedy na zahraničním účtu.

4. **NEKLIKEJTE NA PODEZŘELÉ ODKAZY – NA SPOUSTĚ WEBŮ SE SKRÝVÁ NEBEZPEČÍ –** Ano, samozřejmě … slyšeli jste to stokrát ba co stokrát, tisíckrát. Stačí chvíle nepozornosti a pokles pozornosti a do počítače se Vám usídluje útočník. Stejně tak by uživatelé rozhodně neměli klikat na bannery, které jim slibují finanční odměnu, nový smartphone zdarma či jinou výhru.

5. **BUĎTE OPATRNÍ I U STRÁNEK S IKONOU ZÁMEČKU -** https:// Rozšířeným mýtem je, že pokud je stránka chráněna (připojení https://) je tato stránka bezpečná, ale to nemusí být pravda. Dnes útočníci dokážou vytvořit stránky se stejným zabezpečením, které ale využívají k šíření nebezpečného softwaru.

6. **NEPODCEŇUJTE PROGRAMY ZOBRAZUJÍCÍ REKLAMU – MOHOU BÝT PŘEDZVĚSTÍ ÚTOKU –** Mnoho uživatelů bere tzv. adware, tedy program zobrazující nevyžádanou internetovou reklamu, na lehkou váhu. Nicméně tyto programy mohou být nebezpečné. Pro útočníky je to nástroj jak o Vás získat cenné informace, které dále použijí k útoku.

7. **NIKDY NIKOMU NEPOSÍLEJTE CITLIVÉ ÚDAJE – HESLO JE JEN VAŠE A BANKA JE K PŘÍSTUPU NA ÚČET NEPOTŘEBUJE -** Vždy přemýšlejte, komu svěřujete číslo své karty či další údaje. Pravidelně kontrolujte úhrady přes internet ve svém bankovnictví. Útočníci Vás také můžou kontaktovat jako „přítel“ z FB s prosbou o převod hotovosti.

8. **RYCHLÉ ODHALENÍ INCIDENTU – ŽÁDNÉ NEZRANITELNÉ ZAŘÍZENÍ NEEXISTUJE -** Organizace se dnes dělí na dva typy – ty hacknuté a ty, které o tom ještě neví. Buďte připraveni za každé situace. Své síly věnujte nejen prevenci, ale i přípravě scénáře „Po útoku". To znamená rychlé odhalení, zjištění rozsahu škod a jejich napravení.

9. **OTESTUJTE REAKČNÍ PLÁN – DŮVĚŘUJ, ALE PROVĚŘUJ! –** Teorie a praxe se mohou diametrálně lišit. Jednou za čas je dobré otestovat váš reakční plán. Vyzkoušet funkčnost záloh a postupů obnovy infrastruktury a jednotlivých služeb vzhledem k novým trendům a technikám útoků hackerů.

10. **KONTROLA ZAŘÍZENÍ A PROCESŮ – ANEB ŠTĚSTÍ PŘEJE PŘIPRAVENÝM –** Bez zpětné vazby fungování pravidel a procesů, není možno pracovat na jejich aktualizaci a vylepšení. Nutností je kontrola nejen jednotlivých procesů vzhledem k aktuální době, ale i kontrola zařízení a jejich bezpečnosti (firewally, routery …), které již nemusí podporovat nejnovější techniky útoků a tím se postupně zvyšuje jejich zranitelnost. Neopomenutelnou položkou je pak plán investic do ICT vzhledem k obnově a modernizaci vybavení.

Kybernetické útoky se staly celosvětově velkým bussinesem. Díky technikám sociálního inženýrství a dalším technikám se k hackerskému útoku stávají náchylné nejen strategické organizace, ale i běžné firmy a v neposlední řadě každý uživatel ICT techniky osobně. Před cca 15-ti lety mohl hacker napadnout více méně jen počítač, dnes se útok dá vést přes wifi pomocí mobilního telefonu či tabletu nebo ukrýt nebezpečný malware do chipu v chytrém televizoru či ve výrobní lince. Další kapitolou je bezpečnost např. zdravotnických přístrojů či pomůcek.

V každém případě je na každém z nás, aby se zamyslel nad mírou rizika pro jeho osobu, firmu či organizaci a zajistit odpovídající ochranu, případně minimalizaci dopadů takovéhoto útoku. Buď sám nebo se můžete obrátit na odborníky:

+ 420 777 246 777

agm.cz & nodesign.cz

VAŠE PROBLÉMY S IT VYŘEŠÍME ! VŽDY !