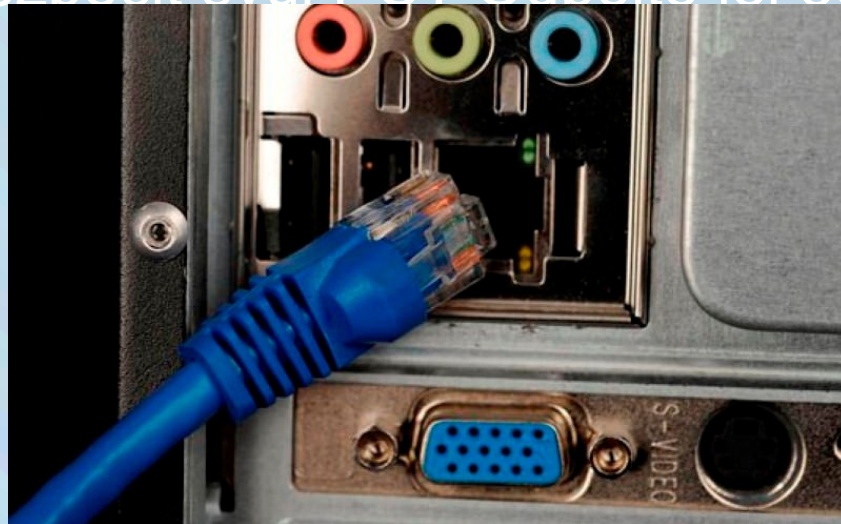


The background features a series of concentric, overlapping circles in shades of blue, teal, and light green, creating a ripple effect. On the left side, there are black circuit-like lines with small circles at their ends, resembling a network or data flow diagram.

OCHRANA POČÍTAČE V POČÍTAČOVÉ SÍTI A ZÁSADY BEZPEČNOSTI PŘI JEHO OBSLUZE

ZABEZPEČENÍ POČÍTAČE

- Řešíme pouze základní zabezpečení PC, ne komplexní zabezpečení sítě
- Jak nejlépe zabezpečit svůj PC? Odpojte jej od internetu



ANTIVIRUS, ANTIMALWARE PROGRAM

- bezpečnostní program, který detekuje, blokuje a odstraňuje kybernetické hrozby.
- Ujistit se zda-li je antivirus správně nastaven a spuštěn
- Jak funguje?
 - detekce charakteristických řetězců (tzv. signatura viru).
 - Analýza zachytávaných dat, sledování aktivity programu
 - Simuluje program a sleduje jeho chování před jeho reálným spuštěním

ADMINISTRÁTOR, UŽIVATEL A OPRÁVNĚNÍ

- Správně nastavená oprávnění
- Oddělení admin a user účtu
 - Založit admin a uživatelský účet (Každý jiné heslo!!!)
 - Při práci používat pouze uživatelský účet
 - Admin účet je využíván pouze tehdy, pokud je ho potřeba např. Instalace SW, změna oprávnění
- Proč? - způsob jakým zamezit útočnickovy volnému "pohybu" v PC

NAME	AUTHORS	VERSION	LATEST VERSION
BareTail	Bare Metal Software, Ltd.	3.50.0.20120226	
Chocolatey	Chocolatey Software, Inc	0.10.11	
Chocolatey Core Extensions	chocolatey	1.3.3	
Chocolatey Licensed Extension	Chocolatey Software	1.12.11	1.12.12 Out Of Date
Chocolatey GUI	Chocolatey	0.17.0-unstable0086	Out Of Date
Dot Net 4.5.2	Microsoft	4.5.2.20140902	
Telerik Fiddler Web Debugger	Telerik	5.0.20182.28034	
LockHunter	Igor Tkachenko, Nikolay Duylovskiy, Cı 3.2		
Squid (Install)	Duane Wessels, Henrik Nordström, Arr 3.5.27		

SPRÁVCE APLIKACÍ

- Je důležité mít přehled v nainstalovaných aplikacích (Při hledání ohroženého SW, aktualizace)
- Správce aplikací udržuje přehled o nainstalovaných aplikacích
- Plošná aktualizace SW

FYZICKÝ PŘÍSTUP K PC

- Zabezpečení fyzického přístupu k počítači
- Zabránění instalace škodlivého hardware (například flashky)
- Zabránění jakékoliv manipulace se zařízením neoprávněné osobě

The background features a series of concentric circles in shades of blue, green, and purple, creating a ripple effect. In the corners, there are stylized circuit board patterns with lines and small circles.

ZÁSADY BEZPEČNOSTI PŘI PRÁCI S POČÍTAČEM

UŽIVATEL JAKO SOUČÁST ZABEZPEČENÍ SÍTĚ

- Každý uživatel a jeho zařízení tvoří důležitou část zabezpečení počítačové sítě
- Napadení 1 uživatele/zařízení může vést k napadení celé sítě
- Každý uživatel je zodpovědný za své chování při práci se svým zařízením
- Největší slabinu v zabezpečení sítě tvoří uživatelé a jejich chyby nikoliv samotná zařízení

HESLA

- Základní zabezpečení: Heslo
- Každý uživatel je zodpovědný za své heslo
- Zásady při vytváření a používání hesel:
 - Síla hesla: Alespoň 8 znaků +, kombinace písmen, číslic a speciálních znaků
 - Nevyužívat slova v heslech (password123, alik12, milacek1)
 - Unikátnost: Nepoužívat stejné heslo na více místech
 - Pravidelné změny hesel
 - Nepoužívat uložení hesel v prohlížeči, hesla si nezapisovat na štítky
- Jak si mám všechna ta hesla pamatovat? - Využití password managementu (1password)

SOCIÁLNÍ INŽENÝRSTVÍ

- Napadení samotného uživatele pomocí různých metod
- (Phising - podvodné e-maily, zprávy, telefoní hovory, internetové stránky, ransomware atd.)
- Jak se bránit?
 - Dávejte si pozor na e-maily – nestahovat neověřené přílohy, posuzujte důvěryhodnost e-mailu (odesílatele)
 - Vzdělávat uživatele/projít si školením - dozvídat se o nových metodách socialního inženýrství
 - Nenavštěvovat nebezpečené, podezřelé webové stránky
 - Nestahovat SW bez ověření zdroje - může se jednat o Malware

SOCIÁLNÍ INŽENÝRSTVÍ - REALNÝ PŘÍKLAD

- Útočník (žena) volala na call centrum společnosti, kde se vydávala za někoho jiného. Pro zvýšení důvěryhodnosti, si do pozadí zapla zvuky pláčícího dítěte a v telefonu zněla uspěchaně a upracovaně.
- Pracovník call centra nechtěl "matku" nechat čekat a snažil se jí co nejlépe a nejrychleji pomoci – dal jí všechny informace co chtěla.
- Jak se měl pracovník call centra správně zachovat?
- Jak se zachováte Vy jakmile se stanete obětí metod sociálního inženýrství?

Od: SERVIS24 <info8347@servis24.com>

Komu:

Odesláno: 22.3.2016 12:57

Předmět: SERVIS 24 byl uzamčen

Chybná E-mailová adresa!

SERVIS•24
INTERNETBANKING

SERVIS 24 byl uzamčen

UKÁZKA PODVODNÉHO E-MAILU

Dosáhli jste maximálního počtu neúspěšných pokusu o přihlášení. Pro Vaši ochranu, přístup k on-line služby je uzamcena.

Chcete-li obnovit váš přístup, kliknout: [Přihlaste se do SERVIS 24](#) a pokračovat v procesu overování.

[SERVIS24 Přihlášení](#) | [Soukromí a bezpečnost](#) | [Kontaktujte nás](#)

AKTUALIZACE SOFTWARE

- Verze SW z pravidla obsahují chyby – zranitelnosti
- Zranitelnost (Vulnerability) - chyba v kódu programu, která způsobuje bezpečnostní problém, kterého může útočník využít (Exploit)
- Pravidelné aktualizace SW (I samotného OS) odstraňují zranitelnosti

ZÁLOHA A SPRÁVNÁ MANIPULACE S DATY

- Důležitost zálohy
- Šifrování dat
- Ochrana před neoprávněnou manipulací s daty (Opravnění)
- Pozor na nešifrované zprávy (e-maily) - veškerou nešifrovanou komunikaci lze zachytit

ZAMYKAT ZAŘÍZENÍ PŘI ODCHODU

- Jednoduchá avšak důležitá zásada

KOMUNIKACE SE SPRÁVCEM SÍTĚ

- Komunikace před incidentem - doptávat se, ujišťovat se
- Informovat správce při pokusu o útok - přišel podvodný mail, někdo zkoušel volat a snaží se získat informace atp.
- Informovat správce po incidentu - nestydět se, přiznat si chybu, oznámit problém dříve než bude pozdě
- Informovat správce o chybách v zabezpečení

SEZNÁMIT SE S BEZPEČNOSTNÍ POLITIKOU PODNIKU A DODRŽOVAT JÍ

- Dobře se s bezpečnostní politikou seznámit
- Dodržovat veškeré postupy, nařízení a zásady
- Pokud musím politiku z nějakých důvodů obejít - zeptat se, zajistit si souhlas, prověřit jiné možnosti

ZÁVĚR

- Při obsluze zařízení zapojeného v podnikové síti nebo u Vás doma používejte selský rozum.
- Často si lidé neuvědomují rizika spojená s bezpečností, dokud se sami nestanou obětí útoku
- Zamyslete se, o co všechno můžete přijít, co všechno můžete Vaším chováním ohrožit