Co-funded by the
Erasmus+ Programme
of the European Union

Kapitola

[Zabezpečení hardwaru a softwaru]

Projekt: B-SAFE
Číslo: 2018-1CZ01-KA204-048148
Jméno autora: EDIT VALUE®
Poslední úprava: 02.09.2020

Co-funded by the
Erasmus+ Programme
of the European Union

Zabezpečení hardwaru a softwaru

Úvod

Hardware a software jsou dvě propojené části počítače, které by bez sebe nemohly fungovat.
Digitalizace přetváří ekonomiku po celém světě. Ať už v práci nebo v našem soukromém životě, vždy se můžeme setkat s nějakými potížemi spojenými s fungováním softwaru či hardwaru, které mají vliv na nás všechny. Pro firmy a celou společnost existují vážná rizika spojená s těmito komponenty, a proto je důležité hardware a software pravidelně aktualizovat, vylepšovat či vyměňovat.
V této kapitole se dozvíte o nejčastějších útocích na hardware a software a jak se před nimi patřičně chránit.
Věděli jste, že většina problémů spojených s užíváním počítače se váže k softwaru? Software počítače může selhat z několika různých důvodů – počítačové viry a napadení malwarem patří mezi ty nejběžnější, jelikož lidé často bezmyšlenkovitě stáhnout nebo kliknou na něco, co má za cíl poškodit Váš počítač. Existuje několik způsobů, jak vyřešit potíže se softwarem, jako jsou jeho odinstalace a opakovaná instalace, vylepšení, používání nejnovějších antivirů či aktualizace softwaru na nejnovější verzi. A to je pouze pár příkladů toho, co můžete dělat. V této kapitole Vám představíme ještě několik dalších.

Praktický význam – K čemu získané znalosti a dovednosti využijete

Nastudováním této kapitoly se dozvíte, jaké existují nejčastější útoky na hardware a software a jaké tipy a doporučení Vám pomohou zlepšit jejich zabezpečení.

Co-funded by the
Erasmus+ Programme
of the European Union

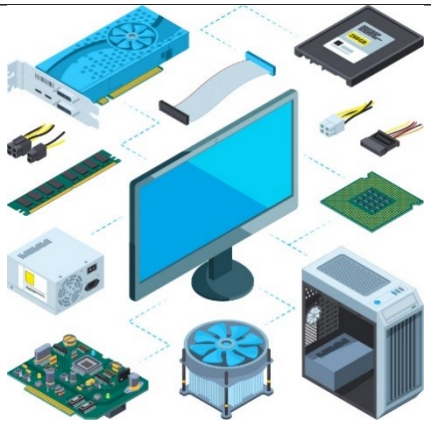
1. Nejčastější druhy útoků na hardware a software

Digitalizace postupně přetváří celý náš svět. Přes velké množství výhod, které tento fenomén přináší, představuje také narůstající riziko pro digitální zabezpečení, které má s neustále zvyšujícím se trendem užívání digitálních zařízení v našem každodenním životě **vzrůstající negativní dopad na bezpečí a soukromí** ať už v našich domovech, autech, zaměstnáních nebo v sítích/na internetu.
Je tedy velmi důležité neustále **aktualizovat, vylepšovat nebo vyměňovat** software a hardware našich zařízení, abychom se vyhnuli potenciálním rizikům a hrozbám, které ovlivňují celou společnosti.

Začněme od nuly: na co vlastně pojmy hardware a software odkazují? V tabulce níže naleznete podrobné definice těchto dvou pojmů.

Definice
Pojmem **hardware** se označuje veškeré fyzické vybavení počítače nebo jiného zařízení, kdežto software je vše, co se nachází uvnitř zařízení – tedy veškeré nainstalované programy v počítači, chytrém telefonu nebo tabletu. Hardware jsou všechny části, z kterých se zařízení skládá, zatímco software shromažďuje a zpracovává data a informace v pevném disku zařízení. Mezi komponenty hardwaru patří například procesor (CPU), pevný disk, základní deska, monitor, tiskárna nebo myš. **Software** je **„logická" část** počítače nebo chytrého telefonu, nelze ho uchopit nebo se ho dotknout, protože je nehmotný. **Všechny softwary ovládají minimálně jeden komponent hardwaru.** Software si můžete představit jako soubor pokynů, které říkají zařízení, co má dělat. Může se jednat o programy nebo data. Například videohry nebo Microsoft Outlook.

Abyste si dokázali rozdíly lépe představit, připravili jsme pro Vás tuto přehlednou tabulku:

	Hardware	Software
		
Funkce	Hardware je **fyzická část** zařízení, ve které dochází ke zpracování dat a informací. Hardware **nemůže fungovat bez softwaru.**	Software je **soubor pokynů**, které říkají počítači, co má dělat. Software **je zodpovědný za fungování hardwaru.**

Charakteristika	Hardware je část zařízení, kterou vidíme a které se můžeme dotknout. Hardware nemůže být napaden počítačovými viry.	Software vidíme a používáme, nemůžeme se ho však dotknout. Software může být **napaden počítačovými viry.**
Životní cyklus	Může dojít k fyzickému poškození hardwaru.	Dochází k stárnutí softwaru, fyzicky se neopotřebuje.
Inicializace	Hardware začne fungovat hned po nainstalování softwaru.	Software je potřeba nainstalovat do hardwaru.
Údržba	Části hardwaru lze přesunout či vyměnit.	Software lze znovu nainstalovat a přemístit.
Příklady	Myš, procesor, monitor, tiskárna, pevný disk atd.	Microsoft Word, Firefox, Skype, Adobe Reader atd.

Jak jste mohli vidět, hardware a software jsou propojené části zařízení a bez softwaru by hardware nemohl fungovat.

V dnešní době je ochrana hardwaru a softwaru velmi aktuálním tématem. Proč tomu tak je? V tabulce níže jsou uvedeny 3 nejvýznamnější přínosy zabezpečení hardwaru a softwaru

Zabezpečení hardwaru	Zabezpečení softwaru
1. Hardware počítače může být velmi křehký (teplo, voda, nesprávné zacházení nebo nehody způsobené lidským zaviněním jsou všechno příklady největších hrozeb pro fyzickou bezpečnost počítače).	**1.** Pravidelné aktualizace softwaru mají plno výhod jako jsou například prevence chyb nebo slabin v programech či operačním systému.
2. Hardware by měl být řádně čistý a chráněný před nadměrným teplem.	**2.** Pravidelné aktualizace softwaru pomáhají vypořádat se s chybami nebo mezerami v zabezpečení.
3. Incidenty jako jsou krádež nebo poškození vodou mohou zapříčinit ztrátu dat a informací a mohou poškodit systém nebo soubory.	**3.** Software pomáhá chránit data a citlivé informace před malwarem a jinými vnějšími hrozbami.

Je tedy zřejmé, že zabezpečení hardwaru a softwaru hraje důležitou roli pro zajištění důvěryhodnosti, integrity a autentičnosti. **Pojďme se podívat na pár příkladů, na kterých je dobře vidět důležitost ochrany a zabezpečení hardwaru a softwaru.**

Příklad
Věděli jste, že v roce 2011 utrpěla společnost Sony Pictures útok od skupiny hacktivistů, kteří zveřejnili kolem 1 milionu uživatelských účtů včetně osobních údajů (hesla, e-maily, adresy bydliště, data narození atd.), což znamenalo porušení zásad ochrany osobních údajů této společnosti? V roce 2017 byla napadena společnost HBO a útočník uveřejnil scénář epizody populárního televizního seriálu (Hra o trůny), která ještě nebyla odvysílána, a také získal přístup k finančním dokumentům, seznamu kontaktů obsazených herců a štábu a k dalším důvěrným informacím.

Co-funded by the
Erasmus+ Programme
of the European Union

Těmto druhům incidentů lze předejít silným zabezpečením softwaru a hardwaru.

1. Procvičte si znalosti

Cvičení /VÍCE MOŽNOSTÍ/

Související dílčí výukový cíl: DVC_Zabezpečení hardwaru a softwaru_01_01: Znáte definice pojmů hardware a software.

Zadání: Co znamenají pojmy hardware a software?
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Software je část počítače, které se lze dotknout.
- Hardware může být napaden počítačovými viry.
- Software je zodpovědný za fungování hardwaru.
- Hardware a software fungují pouze dohromady.

Cvičení /VÍCE MOŽNOSTÍ/

Související dílčí výukový cíl: DVC_Zabezpečení hardwaru a softwaru_01_02: Dokážete vysvětlit přínos zabezpečení hardwaru a softwaru.

Zadání: Vyberte správná tvrzení týkající se zabezpečení hardwaru a softwaru.
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Nejčastější útoky na hardware pocházejí z vnějších zdrojů.
- Zabezpečení softwaru je potřeba provádět pravidelně.
- Útoky na software jsou nejčastější, proto je potřeba použít několik druhů ochrany.
- Software musí být chráněn antivirem.

2. Jak vylepšit zabezpečení hardwaru

Teď když už víte, co je to hardware a software a proč je tak důležité je chránit, je načase abyste se dozvěděli o nejčastějších typech útoků a jak se jim vyhnout. A přesně na to jsou zaměřeny dvě následující podkapitoly.

Následující stránky Vám odhalí nejčastější druhy útoků na hardware a poskytnou Vám užitečné tipy a doporučení ohledně prevence a ochrany.

Nejdříve byste však měli je vědět, co vlastně zabezpečení hardwaru je a jaké jsou nejčastější útoky na hardware.

Co-funded by the Erasmus+ Programme of the European Union

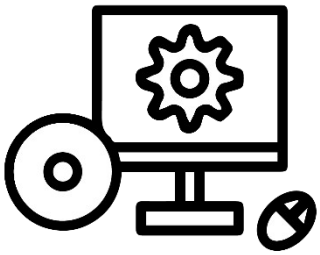
Zabezpečení hardwaru souvisí s **ochranou zařízení po fyzické stránce** a jeho provedení závisí čistě na Vás.

Jaké jsou tedy nejčastější útoky na hardware?

Existují 3 útoky, ke kterým dochází nejčastěji. Dva z nich jsou popsány v následující tabulce:

HARDWARE	
Fyzické nehody	**Modding**
Sem patří nehody jako polití vodou nebo nevhodné zacházení, které zapříčinili lidé. Tento druh poškození představuje problém pro vnější fyzické zabezpečení počítače.	Úprava hardwaru, softwaru nebo čehokoliv jiného za účelem získání funkce, která nebyla původně navržena nebo zamýšlena výrobcem.

Příklady **nejčastějších důsledků útoků na hardware**:

Modding 	**Škodlivé úpravy hardwaru** od znalců představují vážnou hrozbu pro Vaše zařízení. Proto je důležité dobře znát původní zdroj, od kterého si počítačové komponenty pořizujete. Důležité součásti jako například mikroprocesor mohou být uvnitř počítače upraveny tak, aby Vám uškodily.
Fyzické nehody 	Hardware může být velmi křehký a také velmi cenný. Horko, vlhkost, vibrace, teplotní extrémy, prach, voda a fyzické nehody představují největší riziko pro fyzickou bezpečnost komponentů a celého počítače. Proto je důležité udržovat veškeré části hardwaru čisté, daleko od zdrojů nadměrného tepla a nemanipulovat s tekutinami v jejich blízkosti.

Teď, když už víte, co všechno se může s Vaším hardwarem stát, jistě uvítáte nějaké rady a tipy, jak takovýmto situacím předejít a udržet Váš hardware v bezpečí.

V následujících bodech se dozvíte **pár užitečných kroků**, které Vám s ochranou Vašeho hardwaru pomůžou:

1. V případě, že jste s nimi nesouhlasili, jsou **úpravy hardwaru nelegální.** Je možné, že budete chtít provést nějaké úpravy za účelem zlepšení Vašeho počítače (zvýšit rychlost, zvětšit paměť atd.). Proto je nesmírně důležité **vyhnout se nákupu komponentů hardwaru od nedůvěryhodných zdrojů** jako jsou online platformy, které nejsou příliš známé mezi širokou

veřejností a které lákají na své nízké a často nereálné ceny. Hardware zakoupený od takovýchto prodejců může představovat velikou hrozbu pro Vaše bezpečí;

2. Dále existují **speciální sledovací systémy**, které Vám pomohou s dohledáním Vašeho hardwaru, pokud dojde například k jeho krádeži nebo ztrátě;
3. Abyste svému hardwaru poskytli jen tu nejlepší péči, je důležité mít vždy **nainstalovaný a aktualizovaný bezpečnostní software.** Tento tip je více rozveden v následující kapitole;
4. **Vyvarujte se pokládání hardwaru na vysoká místa, blízko zdrojů tepla, vody a elektrických obvodů;**
5. **Vyčistěte hardware velmi jemně suchým hadříkem** nebo speciálním nástrojem k tomu určeným, jako je například kartáč s dlouhou rukojetí a jemnými štětinami nebo ubrousky dostupné ve speciálních obchodech zaměřených na elektroniku. Zapamatujte si tento tip jako pravidlo pro údržbu a používejte jej podle potřeby.

2. Procvičte si znalosti

Cvičení /VÍCE MOŽNOSTÍ/

Související dílčí výukový cíl: DVC_Zabezpečení hardwaru a softwaru_02_01: Dokážete vysvětlit, co je to zabezpečení hardwaru.

Zadání: **Co si lze představit pod pojmem zabezpečení hardwaru?**
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Zabezpečení hardwaru závisí pouze na lidech.
- Zabezpečení hardwaru se vztahuje k ochraně fyzických částí zařízení.
- Na zabezpečení hardwaru nestačí pouze jedna osoba.
- Zabezpečení hardwaru souvisí pouze se zavedením fyzických opatření.

Cvičení /VÍCE MOŽNOSTÍ/

Související dílčí výukový cíl: DVC_Zabezpečení hardwaru a softwaru_02_02: Dokážete popsat hlavní důsledky útoků na hardware.

Zadání: **Vyberte správná tvrzení ohledně ohrožení zabezpečení hardwaru.**
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Nejčastější druh útoku na hardware souvisí s neoprávněnými fyzickými úpravami.
- K fyzickým nehodám dochází kvůli lidské lehkomyslnosti a nezodpovědnosti.
- Útoky na hardware mohou ohrozit osobní údaje a fyzické bezpečí majitele.
- Útoky na hardware souvisí s úpravami a fyzickými nehodami.

Cvičení /VÍCE MOŽNOSTÍ/

Související dílčí výukový cíl: DVC_Zabezpečení hardwaru a softwaru_02_03: Dokážete popsat tipy a doporučení, jak předejít útokům na hardware a jak ho před těmito útoky chránit.

Zadání: **Která opatření lze zavést pro zvýšení zabezpečení hardwaru?**

Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

1. Udržujte hardware čistý a daleko od zdrojů vody a tepla.
2. Zabezpečení hardwaru by mělo být doplněno o zabezpečení softwaru.
3. Nenakupujte hardwarové součástky od pochybných prodejců a vyhněte se tak nechtěným úpravám.
4. Je možné využít speciální sledovací systémy nebo v případě potřeby autodestrukční zařízení.

3. Jak vylepšit zabezpečení softwaru

Nyní se přesuneme k softwaru, jehož zabezpečení je také ohrožováno velkým množstvím potenciálních rizik. V dnešní době všichni používáme rozličné typy softwarů a kolikrát si toho ani nejsme vědomi.

Důležité je tedy kromě definice zabezpečení hardwaru znát také definici zabezpečení softwaru.

Zabezpečení softwaru je **výstavba a metodika ochrany počítačové sítě,** která kombinuje bezpečnostní zařízení s defenzivní ochranou před (vnitřními i vnějšími) zdroji. Ochrana softwaru vyžaduje kombinaci technik souvisejících s odlišným softwarem. Správné a dostatečné zabezpečení softwaru je důležité nejen pro firmy, ale i pro jednotlivce.

Které způsoby útoků na software jsou nejčastější?

Přestože existuje velké množství různých hrozeb, vybrali jsme pro Vás ty nejčastější a přiblížili Vám je v následující tabulce.

SOFTWARE			
Trojský kůň	**Malware**	**Počítačový vir**	**Phishing**
Počítačový program, který získá přístup k počítači nebo systému tak, že se vydává za běžný program. Jeho cílem je způsobit škody v systémových procesech nebo poškodit data na pevném disku atd. Nejčastěji se šíří prostřednictvím e-mailových příloh.	Sem patří spyware, ransomware, počítačové viry nebo počítačoví červi. Malware se nejčastěji dostane do počítače rozkliknutím podezřelého odkazu nebo otevřením přílohy e-mailu a následným nainstalováním nebezpečného programu.	Počítačový program, který má za úkol nakazit jiné programy a zničit důležitá systémová data a znefunkčnit sítě.	Rozesílání podvodných zpráv nejčastěji prostřednictvím e-mailů, které se zdají být z důvěryhodného zdroje. Cílem je ukrást osobní údaje a data (údaje o kreditní kartě, přihlašovací údaje atd.).
Ransomware	**Počítačový červ**	**Spyware**	**Cryptojacking**
Zabraňuje přístupu ke	Druh malwaru, který	Software, který	Neoprávněné použití

klíčovým částem sítě.	se dokáže sám množit a šířit na další počítače.	umožňuje útočníkům získat informace o aktivitách počítače.	cizího počítače k těžbě kryptoměny. Útočníci ke cryptojackingu využívají škodlivé odkazy v e-mailech, zavirované webové stránky nebo online reklamu.

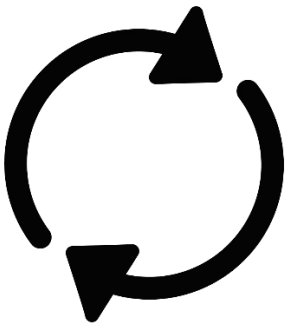
Příklady **nejčastějších důsledků útoků na software**:

Chyby	Častá příčina závad v zabezpečení softwaru. Některé chyby představují slabiny v zabezpečení a mohou mít za následek únik informací nebo neoprávněný přístup.
Poškození ověřování a selhání ochrany dat	Někdy se může stát, že funkce související s ověřováním vyhodnotí situaci nesprávně a dojde k problémům se zabezpečením. To může vést k tomu, že neoprávněné osoby získají přístup k Vašim účtům a následně dojde ke ztrátě důležitých podnikových dat a krádeži osobních údajů, které mohou být použity k poškození Vás nebo Vašich klientů.
Narušení obchodních aktivit	Útok na software může přivést Váš podnik k bankrotu a poničit důvěru zákazníků ve Vaše služby.

Nyní už víte, na jaké nejčastější útoky si dávat pozor, a proto je dalším logickým krokem povědět Vám, co můžete udělat, abyste těmto typům incidentu zabránili.

Níže najdete několik **tipů a doporučení**, jak se vyhnout útokům na Váš software:

	Zabezpečte svoje osobní údaje užíváním **několika různých silných hesel a pravidelným zálohováním.** Dále své informace můžete také šifrovat. Vytvořte **několik záloh svých nejdůležitějších dat** a ujistěte se, že je nemáte všechny uloženy na jednom místě. Vždy mějte **zapnutý firewall**. Učiníte tak v nastavení Vašeho počítače. Pouze firewall ale k ochraně nestačí, proto si také stáhněte ověřený antivirový program.

	**Pravidelně instalujte aktualizace softwaru.** **Nainstalujte si anti-phishingový filtr** na e-mailového klienta a webový prohlížeč. Tyto nástroje nejsou stoprocentní, snižují však počet pokusů zmocnit se Vašich informací. Mějte neustále **aktualizovaný operační systém a bezpečnostní software.** Provádějte **pravidelné antivirové kontroly** a ujistěte se, že Váš antivir a anti-spyware jsou kompatibilní.
	**Nikdy neotevírejte přílohy e-mailů** a nespouštějte programy, pokud si nejste stoprocentně jisti, že pocházejí od důvěryhodného zdroje. **Ověřte si SSL protokol** webové stránky a **nikdy nezadávejte své osobní údaje** na stránce, která nemá platný SSL certifikát. Pro ověření klikněte na visací zámek vedle vyhledávacího řádku. **Vyhněte se užívání veřejných sítí.** **Použijte webový filtr** k blokování nevhodných a škodlivých stránek. Filtr Vám pomůže v kontrole webových stránek vytvořením seznamu povolených nebo blokovaných webů. Návod, jak na to, naleznete zde: www.currentware.com/web-filter.

Nejlepší ochranou před potížemi se softwarem je tedy **prevence** a proaktivní přístup.
Na závěr je důležité si uvědomit, že taktiky útočníků se vyvíjí a zlepšují každý den, a proto je důležité **zůstat v obraze co se týče nejnovějších způsobů útoků a ochranných opatření.** Cílem je být informovaný o aktuálních hrozbách a správném postupu pro zachování bezpečnosti.

3. Procvičte si znalosti

Cvičení /VÍCE MOŽNOSTÍ/

Související dílčí výukový cíl: DVC_Zabezpečení hardwaru a softwaru_03_01: Dokážete vysvětlit, co je to zabezpečení softwaru.

Zadání: **Co si lze představit pod pojmem zabezpečení softwaru?**
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Zabezpečení softwaru vyžaduje kombinaci několika metod a technik.

- Zabezpečení softwaru je převážně reaktivní.
- Zabezpečení softwaru je nutné provádět častěji než zabezpečení hardwaru.
- Zabezpečení softwaru je důležitější, protože lidé se softwarem pracují denně.

Cvičení /VÍCE MOŽNOSTÍ/

Související dílčí výukový cíl: DVC_Zabezpečení hardwaru a softwaru_03_02: Dokážete popsat hlavní důsledky útoků na software.

Zadání: Jaké jsou následky útoků na software?
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Únik informací.
- Neoprávněný přístup.
- Finanční ztráta.
- Poškození ověřování a selhání ochrany dat.

Cvičení /VÍCE MOŽNOSTÍ/

Související dílčí výukový cíl: DVC_Zabezpečení hardwaru a softwaru_03_03: Dokážete popsat tipy a doporučení, jak předejít útokům na software a jak ho před těmito útoky chránit.

Zadání: Jaká opatření týkající se zabezpečení softwaru je možno zavést?
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Je nutné používat několik druhů zabezpečení a pravidelně provádět výkonnostní testy.
- Aktualizovaný firewall, antivirus a phishingový filtr.
- Útoky na zabezpečení softwaru se stávají složitějšími, a proto je potřeba jim přizpůsobovat metody ochrany.
- Protože se softwarové útoky neustále vyvíjejí, opatření na ochranu softwaru by měla být také pravidelně aktualizována.

Zdroje

Diana, J. (n.d.). *Hardware e Sorfware.* https://www.todamateria.com.br/hardware-e-software/

Hossain, F. R. (July 4 2018). *Importance of Security in Software Development.* Retrieved from https://medium.com/brainstation23/importance-of-security-in-software-development-f92669838a90

Zapamatujte si

Shrnutí

Co-funded by the
Erasmus+ Programme
of the European Union

Zabezpečení hardwaru a softwaru je nezbytnou součástí ochrany soukromí a je **zodpovědné za uchování cenného softwarového majetku, který je ohrožován všemožnými škodlivými aktivitami.**

Přestože je **hardware a software propojen** a jeden bez druhého by nemohl fungovat, jedná se o dvě odlišné věci. **Hardware** je **fyzická část**, která se nachází v zařízení nebo se používá spolu se zařízením, kdežto **software** je **logická část** zařízení. Příklady hardwaru jsou například základní deska, monitor, tiskárna nebo myš a příklady softwaru jsou videohry nebo programy jsou Microsoft Office.

Ačkoliv je nemožné se úplně vyhnout incidentům spojeným s poškozením zabezpečení hardwaru či softwaru, existuje celá řada opatření či nástrojů, které Vám pomohou s prevencí těchto incidentů. **Hardware nejčastěji čelí lidským chybám** jako jsou poškození v důsledku nesprávného zacházení, nedostatečné péče nebo vystavování vnějším vlivům (voda, teplo, chlad atd.). **Software** je vystavován vnějším digitálním hrozbám jako jsou **kybernetické útoky** v podobě trojského koně, virů, phishingových útoků, spywaru, malwaru a dalších. Proto je velmi důležité zavedení preventivních opatření, aby se riziko těchto útoků co nejvíce snížilo. Jedním z nejzákladnějších doporučení je používat **několik silných hesel a pravidelně provádět zálohy**, používat **nejnovější verze firewallu a antivirového programu a filtr na prohlížeč,** který zablokuje škodlivé stránky.

Jak vidíte, **prevence je klíčem** k zamezení problému se softwarem, a proto je dobré být proaktivní. Jinými slovy, pokud budete jednat dopředu, pravděpodobně se vyhnete nechtěným problémům a nežádaným následkům.

Na závěr je důležité mít na paměti, že útočníci neustále vylepšují své metody, a proto je důležité **zůstat v obraze ohledně nejnovějších způsobů zabezpečení a ochranných opatření.**

Co-funded by the
Erasmus+ Programme
of the European Union

1. Procvičte si znalosti

Zadání: Co znamenají pojmy hardware a software?
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Software je část počítače, které se lze dotknout.
- Hardware může být napaden počítačovými viry.
- Software je zodpovědný za fungování hardwaru.
- Hardware a software fungují pouze dohromady.

Zadání: Vyberte správná tvrzení týkající se zabezpečení hardwaru a softwaru.
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Nejčastější útoky na hardware pocházejí z vnějších zdrojů.
- Zabezpečení softwaru je potřeba provádět pravidelně.
- Útoky na software jsou nejčastější, proto je potřeba použít několik druhů ochrany.

Software musí být chráněn antivirem.

Zadání: Co si lze představit pod pojmem zabezpečení hardwaru?
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Zabezpečení hardwaru závisí pouze na lidech.
- Zabezpečení hardwaru se vztahuje k ochraně fyzických částí zařízení.
- Na zabezpečení hardwaru nestačí pouze jedna osoba.
- Zabezpečení hardwaru souvisí pouze se zavedením fyzických opatření.

Zadání: Vyberte správná tvrzení ohledně ohrožení zabezpečení hardwaru.
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Nejčastější druh útoku na hardware souvisí s neoprávněnými fyzickými úpravami.
- K fyzickým nehodám dochází kvůli lidské lehkomyslnosti a nezodpovědnosti.
- Útoky na hardware mohou ohrozit osobní údaje a fyzické bezpečí majitele.
- Útoky na hardware souvisí s úpravami a fyzickými nehodami.

Zadání: Která opatření lze zavést pro zvýšení zabezpečení hardwaru?
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

5. Udržujte hardware čistý a daleko od zdrojů vody a tepla.
6. Zabezpečení hardwaru by mělo být doplněno o zabezpečení softwaru.
7. Nenakupujte hardwarové součástky od pochybných prodejců a vyhněte se tak nechtěným úpravám.

8. Je možné využít speciální sledovací systémy nebo v případě potřeby autodestrukční zařízení.

Zadání: Co si lze představit pod pojmem zabezpečení softwaru?
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Zabezpečení softwaru vyžaduje kombinaci několika metod a technik.
- Zabezpečení softwaru je převážně reaktivní.
- Zabezpečení softwaru je nutné provádět častěji než zabezpečení hardwaru.
- Zabezpečení softwaru je důležitější, protože lidé se softwarem pracují denně.

Zadání: Jaké jsou následky útoků na software?
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Únik informací.
- Neoprávněný přístup.
- Finanční ztráta.
- Poškození ověřování a selhání ochrany dat.

Zadání: Jaká opatření týkající se zabezpečení softwaru je možno zavést?
Úkol: Vyberte správné odpovědi: žádná, jedna, jedna a více nebo všechny odpovědi mohou být správně.

- Je nutné používat několik druhů zabezpečení a pravidelně provádět výkonnostní testy.
- Aktualizovaný firewall, antivirus a phishingový filtr.
- Útoky na zabezpečení softwaru se stávají složitějšími, a proto je potřeba jim přizpůsobovat metody ochrany.
- Protože se softwarové útoky neustále vyvíjejí, opatření na ochranu softwaru by měla být také pravidelně aktualizována.