OSVĚTA V OBLASTI KYBERNETICKÉ BEZPEČNOSTI

Martin Hájek

Národní úřad
pro kybernetickou
a informační bezpečnost

Kybernetická bezpečnost v ČR

2011	NBÚ ustanoven jako gestor KB Národní centrum kybernetické bezpečnosti
2012	Národní strategie kybernetické bezpečnosti I.
2015	Zákon o kybernetické bezpečnosti Národní strategie kybernetické bezpečnosti II.
2016	Směrnice NIS
2017	Novela zákona NÚKIB

NBÚ

nckb

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

- **Ústřední správní orgán pro:**
- KYBERNETICKOU BEZPEČNOST
- ochranu utajovaných informací v oblasti informačních a komunikačních systémů
- kryptografickou ochranu
- **ÚŘAD VZNIKL 1.8.2017**

SLUŽBY Úřadu v kybernetické bezpečnosti:

- provozování Vládního CERT České republiky (GovCERT.CZ)
- příprava bezpečnostních standardů
- ochrana utajovaných informací v oblasti IS/KS
- kryptografická ochrana
- cvičení kybernetické bezpečnosti
- **osvěta a podpora vzdělávání**
- výzkum a vývoj

OSTATNÍ DŮVODY:
- zero day, phishing, backdoor...

LIDSKÁ CHYBA:
- špatná konfigurace systému
- neaktualizované aplikace
- použití defaultních přihlašovacích údajů
- použití slabých hesel
- ztracené notebooky a telefony
- vyzrazení citlivých informací skrze chybné emailové adresy

PRIMÁRNÍ CÍLOVÁ SKUPINA:

PRACOVNÍCI
STÁTNÍ SPRÁVY
& SAMOSPRÁVY

ZAMĚSTNANCI
STRATEGICKÝCH
PODNIKŮ

ENTITY
PODLE ZKB & NIS

SEKUNDÁRNÍ CÍLOVÁ SKUPINA

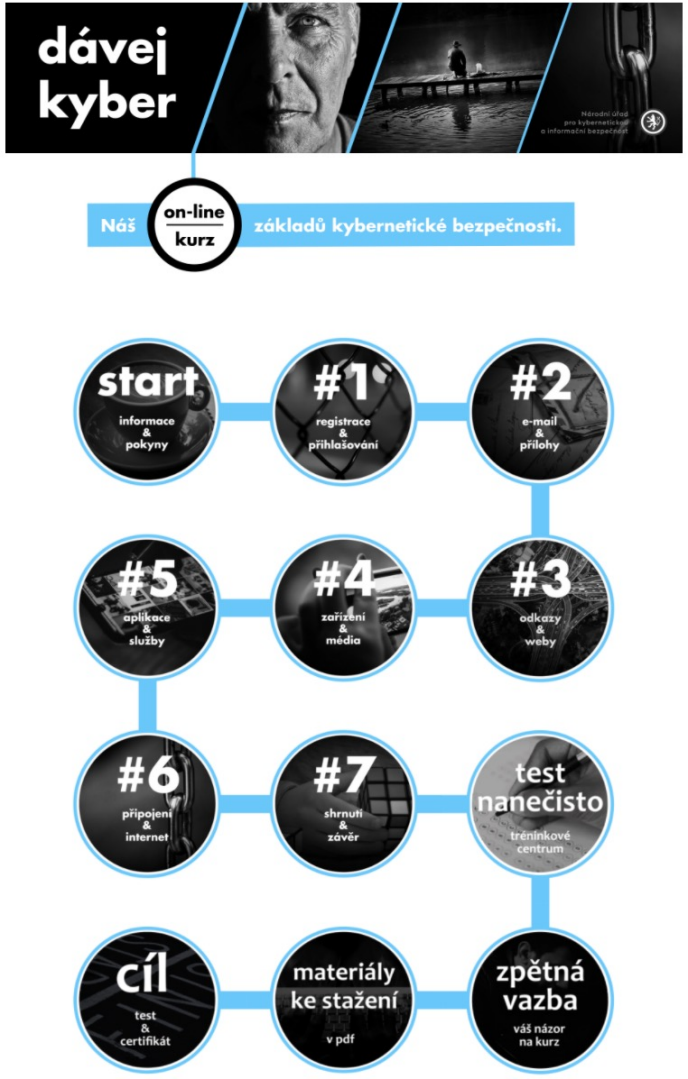
ŽÁCI
& UČITELÉ

PRACOVNÍCI
PREVENCE

POLICIE

SENIOŘI

ONLINE KURZY



Kurz základů kybernetické bezpečnosti

6 okruhů, závěrečný test & certifikát o absolvování

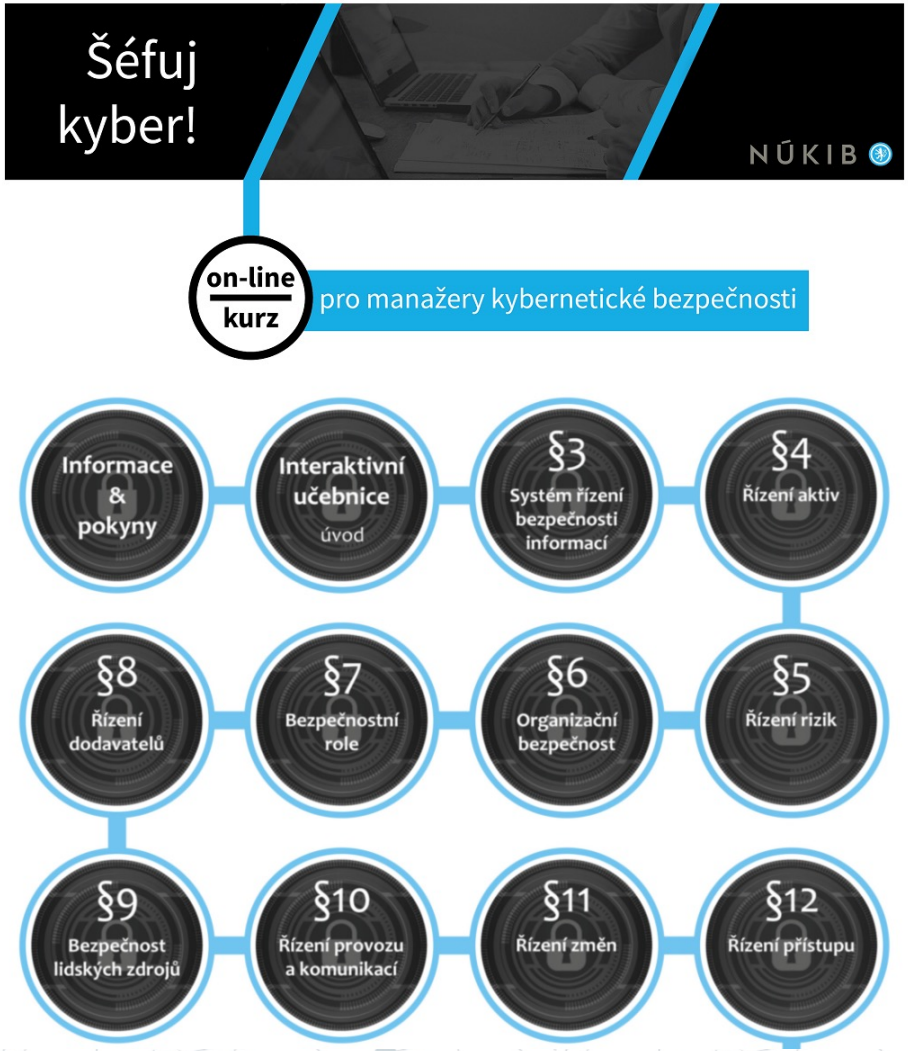
3. verze kurzu

víc než 70 000

vydaných certifikátů

Odběratelé obsahu kurzu

- Armáda ČR
- Zpravodajské služby
- Svaz průmyslu a dopravy
- Českomoravská konfederace odborových svazů
- České dráhy
- Moravská zemská knihovna



Kurz pro manažery kybernetické bezpečnosti

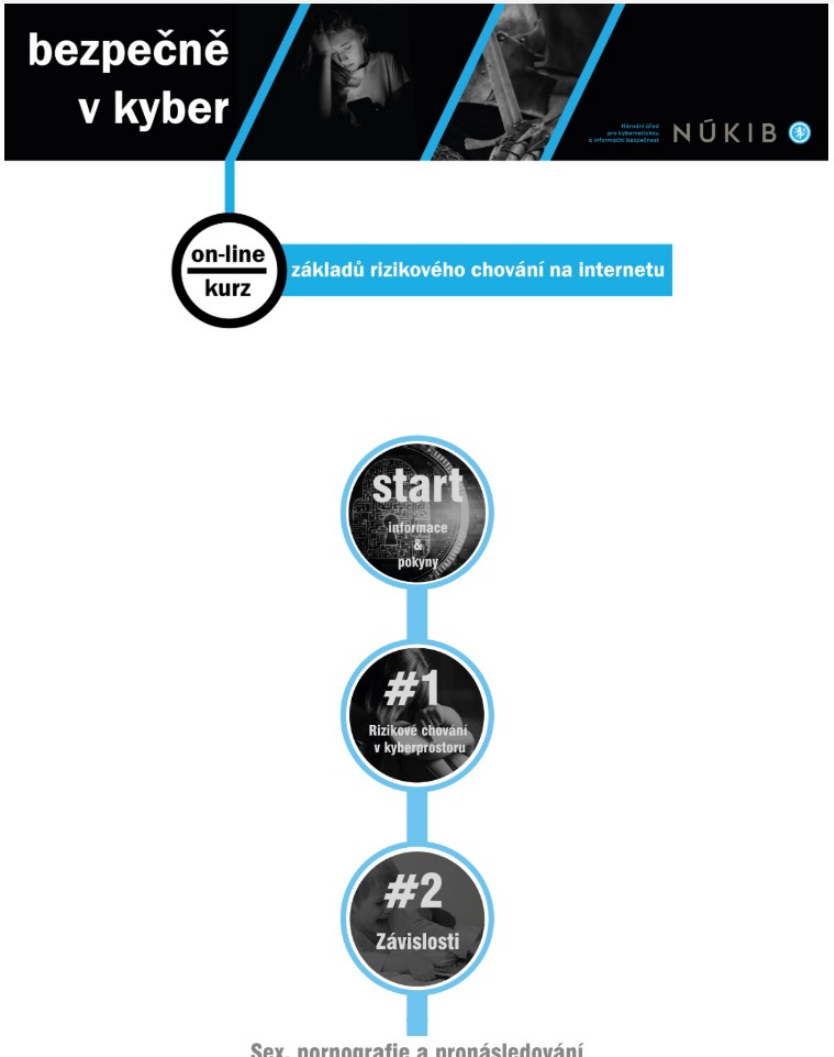
2. verze kurzu

interaktivní učebnice & workshop

seznámení s Vyhláškou o kybernetické bezpečnosti

víc než 950

vydaných certifikátů



On-line kurz základů rizikového chování na internetu

7 okruhů, závěrečný test
& certifikát o absolvování

2. verze kurzu

víc než 3500
vydaných certifikátů

Tematické okruhy kurzu

- Rizikové chování
- Závislosti
- Sexting
- Kybergrooming
- Kyberstalking
- Kyberšikana
- Agrese, sociální bubliny, a další…

Odběratelé obsahu kurzu

- školní metodikové prevence
- policejní preventisté
- pedagogové, koordinátoři ICT
- pracovníci OSPOD, PMS - týmů pro mládež
- linioví pracovníci,
- neziskový sektor,
- studenti VŠ

PROSTŘEDKY PRO WEBINÁŘE

ANTIPHISHING MODUL

Nastavení emailů

Filtr

Název	Obsahuje		Předmět	Obsahuje	
Email	Obsahuje		Vytvořeno	Je shodný	YYYY-MM-DD HH:II:SS
Upraveno	Je shodný	YYYY-MM-DD HH:II:SS			

Filtrovat Vyprázdnit

Název	Předmět	Email	Vytvořeno	Upraveno	Akce
COVID-19	Nepropásněte-Očkování na C-19 ke VŠEM zájezdům pro naše zákazníky	posta@dolovena.cz	12. 03. 2021, 09:49	30. 09. 2021, 10:43	Upravit Odstranit
VOLBY 2021	Chystáte se k voblám?		12. 03. 2021, 10:04	—	Upravit Odstranit

Upravit

Název: COVID-19

Předmět: Nepropásněte-Očkování

Email

Dobrý den,

chystáte se i přes aktuální situaci na podzimní dovolenou nebo služební cestu a nemáte ještě očkování proti COVID-19? Naše společnost získala **po dobu jednoho měsíce** výhradní právo na **využití vakcíny** AstroZenica **pro očkování klientů všech věkových kategorií naší cestovní kanceláře**.

Z tohoto důvodu jsme se rozhodli vám nabídnout tuto vakcínu zcela ZDARMA k zájezdu nebo výletu, který si u nás zakoupíte. **Proto neváhejte, nabídka je platná jen jeden měsíc!**

Odesilatel

Jméno: Karel

Příjmení: Nejedlý

Email: posta@dolovena.cz

Výpisy

Filtr

Instituce	Jméno uživatele	Email	Kurz	Název emailu	Datum odeslání	Datum navštívení	Počet navštívení	Datum posl navštívení
NÚKIB - OVVP	Monika Dittmannová	m.dittmannova@nukib.cz	Kyber nemocnice!	COVID-19	07. 06. 2021, 15:00	—	0	—
NÚKIB	Nitram Keják	f482697640cee3318c2778edd4bb0844	Kyber nemocnice!	COVID-19	09. 06. 2021, 04:05	—	0	—
test	Lucie Zavadilová	lucie.zavadilova@pragodata.cz	Cvičiště	Covid 2	10. 06. 2021, 15:15	10. 06. 2021, 13:17	5	11. 06. 2021
test	Alena Zalejská	alena.zalejska@pragodata.cz	Cvičiště	Covid 2	10. 06. 2021, 15:45	10. 06. 2021, 13:45	6	11. 06. 2021
NÚKIB - OVVP	Nina Adamcová	n.adamcova@nukib.cz	Dávej kyber!	Covid 2	15. 06. 2021, 04:05	15. 06. 2021, 06:09	32	12. 09. 2021
NÚKIB - OVVP	Petr Seifert	p.seifert@nukib.cz	Dávej kyber!	Covid 2	15. 06. 2021, 04:05	—	0	—
NÚKIB - OVVP	Petra Sobková	p.sobkova@nukib.cz	Dávej kyber!	Covid 2	15. 06. 2021, 04:05	15. 06. 2021, 05:26	2	15. 06. 2021

OSVĚTOVÉ MATERIÁLY

BEZPEČNÝ POHYB V KYBERSVĚTĚ

JAK SI ZABEZPEČÍM POČÍTAČ NEBO SMARTPHONE?

OMEZÍM PŘÍSTUP DALŠÍCH OSOB K SOUKROMÝM I PRACOVNÍM ZAŘÍZENÍM.

CHRÁNÍM SVÁ DATA PRO PŘÍPAD ODCIZENÍ ČI ZTRÁTY ZAŘÍZENÍ.
Využívám silné heslo, číselný kód, gesto nebo jiný způsob zabezpečení.

NIKDY SI NEUKLÁDÁM PŘIHLAŠOVACÍ ÚDAJE K ZAŘÍZENÍM A ÚČTŮM V JEJICH BLÍZKOSTI.
Pro uchování přihlašovacích údajů používám šifrovaného správce hesel.

UJISTÍM SE, ŽE PŘI ZADÁVÁNÍ PŘIHLAŠOVACÍCH ÚDAJŮ JE NIKDO CIZÍ NEVIDÍ, NAPŘÍKLAD POHLEDEM PŘES RAMENO.

ZAMKNU ZAŘÍZENÍ POKAŽDÉ, KDYŽ OD NĚJ ODCHÁZÍM.
U počítače s Windows je nejjednodušší způsob rychlého zamknutí klávesová zkratka WIN + L a u mobilního zařízení stisknutí vypínacího tlačítka na jeho boku. Pokud odcházím na delší dobu, ukončím správce hesel a všechny doposud používané aplikace a služby s citlivými údaji jako e-mail nebo internetové bankovnictví.

AKTUALIZUJI SOFTWARE A NEVYPÍNÁM PRAVIDELNÉ AUTOMATICKÉ AKTUALIZACE SYSTÉMU.
Díky tomu zajistím opravu známých zranitelností, které by mohly ohrozit mé zařízení.

POUŽÍVÁM AKTUALIZOVANÝ ANTIVIROVÝ SOFTWARE A FIREWALL.

ZAPÍNÁM WI-FI, BLUETOOTH, NFC A DALŠÍ BEZDRÁTOVÉ TECHNOLOGIE, JEN POKUD JE VYUŽÍVÁM.
Pro útočníka představují potenciální cestu do zařízení.

POKUD VYUŽÍVÁM NEZABEZPEČENOU WI-FI SÍŤ, VYUŽÍVÁM TZV. VPN (VIRTUAL PRIVATE NETWORK) NEBOLI VIRTUÁLNÍ SOUKROMOU SÍŤ, KTERÁ ZABEZPEČÍ MOU KOMUNIKACI NA POTENCIÁLNĚ NEBEZPEČNÉ SÍTI.

ŠIFRUJI CITLIVÁ DATA NA EXTERNÍM DISKU A DALŠÍCH PŘENOSNÝCH ZAŘÍZENÍCH.
Tak budou v případě ztráty nebo odcizení nečitelná.

PRAVIDELNĚ ZÁLOHUJI DATA.
Využít mohu například externí disk. Důležité je, aby záloha byla na jiném místě než v mém zařízení, byla šifrována a připojena pouze v okamžiku zálohování.

DO MÝCH ZAŘÍZENÍ NEPŘIPOJUJI NEZNÁMÉ USB FLASH DISKY, EXTERNÍ DISKY A JINÁ PAMĚŤOVÁ ZAŘÍZENÍ.
Mohou obsahovat malware. V případě nutnosti připojit neznámé médium provedu jeho antivirovou kontrolu. Zaměstnavatel může k tomuto účelu poskytnout tzv. antivirovou pračku, tedy počítač bez připojení k internetu, kde je nainstalovaný aktualizovaný antivirový program.

PŘI PROCHÁZENÍ WEBU PREFERUJI WEBOVÉ STRÁNKY ZABEZPEČENÉ POMOCÍ PROTOKOLU HTTPS.
Https protokol poznáme podle zámečku v adresním řádku:

Stránky zabezpečené pomocí HTTPS

https:// Stránky s částečným šifrováním, nebo bez něj. Nedoporučeno pro odesílání citlivých dat.

DÁVÁM POZOR, NA KTERÉ ODKAZY KLIKÁM.
Je-li to technicky možné, zkontroluji, že odkaz nevede na pozdařilou URL adresu. Pokud nemohu ověřit, kam odkaz vede, neklikám na něj.

VYPÍNÁM NEŽÁDOUCÍ SLUŽBY OPERAČNÍHO SYSTÉMU.
Například monitorování polohy, odesílání diagnostických dat, ovládání vzdáleného počítače na dálku, apod.

JAK MÁM SPRÁVNĚ A BEZPEČNĚ KOMUNIKOVAT?

K INFORMACÍM NA INTERNETU PŘISTUPUJI KRITICKY, NEMUSÍ BÝT PRAVDIVÉ.
Při práci s informacemi mohou využít rady, které sepsala iniciativa **ZVOLSI.INFO** ve svém **Surfařově průvodci internetem.**

NEZVEŘEJŇUJI OSOBNÍ ANI CITLIVÉ INFORMACE O MNĚ, MÉ RODINĚ, PŘÁTELÍCH NEBO SPOLUPRACOVNÍCÍCH.
Data narození, náboženské vyznání nebo fotografie mohou být zneužity.

INTIMNÍ FOTOGRAFIE A VIDEA NEVYTVÁŘÍM, NEUMÍSTUJI JE NA INTERNET ANI JE NIKOMU NEPOSÍLÁM.
Nikdy nevím, kdy může být takový materiál zneužit.

PŘI KOMUNIKACI SI VŽDY OVĚŘUJI IDENTITU PROTISTRANY.
Mohu se zeptat přátel nebo si dotyčného vyhledat na internetu. Pokud si nejsem jist, zda mi skutečně volají například z IT oddělení naší instituce, nebo mě po telefonu úkoluje nadřízený, kterého neznám, zavěsím a zavolám zpátky na telefonní číslo z oficiálního seznamu.

NIKDY NEOTEVÍRÁM PHISHINGOVÉ E-MAILY A PODEZŘELÉ PŘÍLOHY A INFORMUJI IT ODDĚLENÍ.
V práci podezřelý e-mail neotevírám a informuji o něm IT oddělení. Stejně tak neotevírám podezřelé přílohy. Pokud mi takový e-mail dorazí do mé osobní schránky, mohu to nahlásit provozovateli schránky.

JAK PHISHING POZNÁM?
"Phishing je podvodná technika, prostřednictvím které se útočníci snaží například získat mé osobní nebo citlivé informace (přihlašovací údaje, datum narození, číslo platební karty atd.), nasměrovat mě na podvodnou stránku, nebo mi zaslat závadnou přílohu. Phishing se nejčastěji šíří formou e-mailových zpráv, které vypadají jako odeslané z důvěryhodných institucí." Podvodník používá obecná oslovení typu „Vážený pane/i" bez uvedeného jména, v textu e-mailu mohou být gramatické, stylistické a grafické chyby, obsahuje podezřelé vyhlížející odkazy typu https://www.abamka.cz.

V KOMUNIKACI NEJSEM ZBYTEČNĚ SDÍLNÝ.
Vše, co na sebe prozradím, může být zneužito.

NENÍ OBĚD ZADARMO A TO ANI V ONLINE SVĚTĚ.
Zpozorním, jsou-li mi zdarma nabízeny jindy placené služby nebo produkty. Pokud za produkt neplatím, jde o má data.

RANSOMWARE JE PROGRAM, KTERÝ ZAŠIFRUJE DATA NEBO CELÝ OPERAČNÍ SYSTÉM A NABÍZÍ JEJICH ZPŘÍSTUPNĚNÍ AŽ PO ZAPLACENÍ VÝKUPNÉHO.
Do zařízení se mi může takový program dostat po otevření neznámé přílohy v e-mailu, z webového prohlížeče nebo tím, že navštívím infikovanou webovou stránku. Před známými druhy ransomware mě chrání aktualizovaný antivirový program. Svá data chráním také pravidelným zálohováním.

PŘI KOMUNIKACI NESPĚCHÁM A VŠE SI PROMYSLÍM.
Útočníci rádi pracují s časovou tísní - teď je třeba něco vykonat, napravit, sdělit. Klidí Škoda z prodlení bývá menší, než důsledky neuvážených činů.

JAK ZABEZPEČÍM MÉ ONLINE ÚČTY?

PŘÍSTUPY K PRACOVNÍM I OSOBNÍM ÚČTŮM SI CHRÁNÍM SILNÝM HESLEM.
Hesla nikdy nepíšu na papírky a nenechávám například na monitoru nebo pod klávesnicí. To platí jak v kanceláři, tak i doma.

U SILNÉHO HESLA ZADÁVÁM ALESPOŇ 12 ZNAKŮ A VÍCE.
Při jeho tvorbě jsem originální a kreativní. Využívám malá a velká písmena, číslice, speciální znaky a další symboly. Mohu si zvolit například unikátní větu nebo souvětí, které si lze snadno zapamatovat.

PRO KAŽDOU SLUŽBU POUŽÍVÁM JINÉ UNIKÁTNÍ HESLO.
To platí u pracovních účtů a zařízení bez výjimky. V soukromí se této zásady držím u služeb, které mohou obsahovat osobní a citlivé informace.

NEVYUŽÍVÁM ONLINE NÁSTROJE ČI SLUŽBY PRO KONTROLU SÍLY HESLA.
Výsledkem může být to, že heslo předám útočníkovi, který si díky tomu doplní vlastní databázi používaných hesel.

PROTOŽE JE OBTÍŽNÉ ZAPAMATOVAT SI VŠECHNA HESLA, VYUŽÍVÁM PRO TA MÉNĚ VYZNAMNÁ SPRÁVCE HESEL.
Ten mi umožňuje bezpečně uložit a spravovat velké množství hesel. Přístup do něj je chráněn jedním silným zastřešujícím heslem ideálně v kombinaci s vícefaktorovým ověřením.

NESDÍLÍM PŘIHLAŠOVACÍ ÚDAJE K VLASTNÍM ÚČTŮM A SLUŽBÁM.
V případě pracovního e-mailu, pracovního intranetu, docházkového systému nebo hesla do počítače může mít takové jednání závažné následky.

U KRITICKÝCH SLUŽEB JAKO ELEKTRONICKÉ BANKOVNICTVÍ, PRACOVNÍ NEBO SOUKROMÝ E-MAIL VŽDY VYUŽÍVÁM VÍCEFAKTOROVOU AUTENTIZACI.
Příkladem může být elektronické bankovnictví, kdy musím přihlášení v prohlížeči potvrdit zadáním kontrolní SMS nebo potvrzením výzvy v mém mobilním telefonu. Pokud se do služby přihlašuji z mobilního telefonu, necham si potvrzovací SMS zaslat na jiné zařízení.

ODDĚLÍM ADMINISTRÁTORSKÝ ÚČET OD BĚŽNÉHO
Administrátorský účet používám pouze pro správu systému. Pro ostatní pracovní aktivity jako odesílání e-mailů nebo procházení webu využívám běžný neprivilegovaný účet.

NEPOUŽÍVÁM KONTROLNÍ OTÁZKY PRO OBNOVENÍ HESLA.
Nepoužívám kontrolní otázky pro obnovení hesla. Nikdy si jako alternativu k heslu nezadávám kontrolní otázky typu: "příjmení třídní učitelky z páté třídy" nebo "nejmenší planeta sluneční soustavy". Podobné informace jsou dohledatelné z veřejných zdrojů, je-li kontrolní otázka povinná, chovám se k ní jako k heslu a volím ji tak, aby nebyla dohledatelná. Např. k otázce „Jaké bylo vaše jméno za svobodna" zvolím odpověď „N9qyS_@79b7G&_tp".

www.nukib.cz

Národní úřad pro kybernetickou a informační bezpečnost

BEZPEČNÝ POHYB V KYBERSVĚTĚ

Zaměřeno na:

- počítač & smartphone,
- online komunikaci,
- online účty.

Dvě formy:

- plakát,
- brožura.

BEZPEČNOSTNÍ DOPORUČENÍ NÚKIB PRO ADMINISTRÁTORY 3.0

INFRASTRUKTURA

ČLEŇTE SÍŤ NA MENŠÍ CELKY (SEGMENTACE)
A STRIKTNĚ ODDĚLUJTE UŽIVATELSKÁ PRÁVA NAPŘÍČ UŽIVATELI (SEGREGACE)
s cílem oddělit citlivé informace a kritické služby typu autentizace uživatelů (např. Microsoft Active Directory) a vytvořit zóny s různou úrovní bezpečnostních omezení. stávajících souborů nebo změn konfigurace.

BLOKUJTE ŠKODLIVÉ IP ADRESY A DOMÉNY NA ÚROVNI GATEWAY (BLACKLISTY),
včetně dynamických a jiných domén poskytovaných zdarma anonymním uživatelům Internetu.

NASAĎTE SÍŤOVÉ SYSTÉMY DETEKCE / PREVENCE PRŮNIKU (IDS/IPS)
používající signatury a heuristiky k identifikaci anomálního provozu v rámci sítě i překračujícího perimetr.

SLEDUJTE SÍŤOVÝ PROVOZ
pomocí vybraných síťových prvků nebo rozmístěním dedikovaných síťových sond. Sledujte komunikaci mezi klienty a servery, komunikaci klientů do Internetu, komunikaci mezi servery i provoz na perimetru sítě a identifikujte provozní a bezpečnostní problémy.

UCHOVÁVEJTE SÍŤOVÝ PROVOZ
z úst kritických pracovních stanic a serverů a provoz překračující perimetr sítě pro případné forenzní zkoumání po průniku do sítě a systémů. Záznamy síťového provozu doporučujeme uchovávat po dobu minimálně 12 měsíců, více podle místních okolností a významu sítě – v případě kritické informační infrastruktury (KII) a u informačních systémů základní služby (PZS) podle zákona o kybernetické bezpečnosti a návazných vyhlášek je minimální lhůta 18 měsíců. V případě sítí strategického významu zvažte i možnost automaticky aktivovaného plného záznamu datového provozu (PCAP), a to jak na primárních, tak záložních systémech (např. webových nebo systémových serverech).

KONTROLUJTE PŘÍCHOZÍ E-MAILY
pomocí mechanismů Sender ID, SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) a DMARC (Domain-based Message Authentication, Reporting and Conformance) a blokujte podvržené zprávy. Tyto mechanismy nastavte i pro možnou kontrolu odchozích zpráv druhou stranou.

POUŽÍVEJTE ŠIFROVANÉ SPOJENÍ MEZI POŠTOVNÍMI SERVERY (TLS)
pro zajištění důvěrnosti e-mailové komunikace. Kontrolu obsahu provádějte až poté, co je e-mailový provoz dešifrován.

PROVÁDĚJTE AUTOMATIZOVANOU DYNAMICKOU ANALÝZU OBSAHU E-MAILŮ A WEBU
prováděnou v sandboxu – hledejte podezřelé chování podle síťového provozu, tvorby nových souborů, úpravy stávajících souborů nebo změn konfigurace.

VYUŽIJTE APLIKAČNÍ FIREWALL
k blokování komunikace jiných než povolených aplikací (whitelisting) a blokování nestandardního provozu. V případě koncových stanic blokujte také spojení iniciovaná jinou stranou.

KONTROLUJTE POUŽÍVANÉ CERTIFIKÁTY
především pro SSH autentizaci, webové servery, vzdálenou plochu apod. Kde je to možné, použijte šifrovanou komunikaci.

ZAJISTĚTE CENTRALIZOVANÉ A ČASOVĚ SYNCHRONIZOVANÉ LOGOVÁNÍ SÍŤOVÝCH UDÁLOSTÍ
(povolených a blokovaných) s okamžitým automatickým vyhodnocováním a uložením po dobu minimálně 18 měsíců, více podle místních okolností a významu sítě.

VOLTE JEDNODUCHÉ DOMÉNOVÉ NÁZVY
aby byly jasně viditelné případné záměny písmen ve phishingových e-mailech.

APLIKUJTE WHITELISTING WEBOVÝCH DOMÉN
pro všechny domény – pokud to dovoluje charakter práce uživatelů. Tento přístup je účinnější než blacklistovat malá procenta škodlivých domén.

NASAĎTE ANTI-DDOS TECHNOLOGIE,
které můžete po důkladné úvodní analýze řešit buď vlastními silami, nebo ve spolupráci s poskytovatelem internetového připojení. Anti DDoS ochranu nasaďte na kompletní IP rozsahy vaší organizace.

VYPRACUJTE DISASTER RECOVERY PLAN (DRP)
a mějte připravené správné a funkční emailové adresy a telefonní čísla na ostatní administrátory, nadřízené pracovníky a CERT/CSIRT týmy.

STANICE & SERVERY

UDRŽUJTE AKTUÁLNÍ OPERAČNÍ SYSTÉM
pravidelnými aktualizacemi a v co nejkratší době aplikujte všechny vydané bezpečnostní záplaty.

UDRŽUJTE AKTUÁLNÍ SOFTWARE,
pravidelně kontrolujte verze instalovaného softwaru. U neaktuálního softwaru provedťe v rámci možností update. Zastaralé mohou být i verze použitých doplňků či modulů nebo firmware zařízení.

NEPOUŽÍVEJTE NEPODPOROVANÉ PRODUKTY,
používejte pouze produkty (software i operační systémy), pro které jsou dostupné bezpečnostní záplaty.

OVĚŘUJTE IDENTITU APLIKACÍ A SOUBORŮ
a povolte jen ty důvěryhodné včetně skriptů a DLL knihoven. V prostředí Windows použijte Device Guard, AppLocker, popřípadě Zásady omezení softwaru (SRP).

HARDENING KONFIGURACE UŽIVATELSKÝCH APLIKACÍ
povolte jen funkcionalitu, která je vyžadována pro práci uživatelů. Dodatečné funkce (např. Java a Flash ve webovém prohlížeči, makra v MS Office) povolte pouze, je-li to nutné.

POUŽÍVEJTE OBECNÉ PREVENTIVNÍ MECHANISMY,
které mohou pomoci ochránit systém před zero-day zranitelnostmi, jako např. DEP (Data Execution Prevention), ASLR (Address Space Layout Randomization) nebo SELinux v linuxových systémech.

AKTIVUJTE IDS/IPS SYSTÉMY NA KONCOVÝCH STANICÍCH
detekující anomální chování jako např. injekci kódu do jiných procesů, změnu chráněných registrových klíčů, zachytávání stisků kláves, načítání neznámých ovladačů, snahu o zajištění perzistence a další.

ZAJISTĚTE CENTRALIZOVANÝ SYSTÉM LOGOVÁNÍ UDÁLOSTÍ NA STANICÍCH A SERVERECH,
a to jak úspěšných tak neúspěšných, který bude časově synchronizován např. ze sítě a bude logy okamžitě automaticky vyhodnocovat. Doporučujeme logy událostí ukládat po dobu minimálně 18 měsíců, více podle místních okolností a významu systému.

FILTRUJTE OBSAH E-MAILŮ A PROPOUŠTĚJTE POUZE RELEVANTNÍ DRUHY PŘÍLOH
po důkladné analýze chování uživatelů určete typy souborů, které potřebují posílat e-mailem. Ostatní formáty příloh blokujte – především spustitelný kód. Dále ověřujte soulad přípony souboru a jeho skutečného formátu.

PRAVIDELNĚ ZÁLOHUJTE DŮLEŽITÁ A CITLIVÁ DATA
jako např. obsah webového serveru, databází nebo konfigurací služeb. Pravidelně testujte, zda jsou zálohy funkční a je možné z nich data obnovit.

ZAVEĎTE STANDARD OPERATING ENVIRONMENT (SOE)
se standardizovanou konfigurací pro pracovní stanice (servery), kde budou vypnuty všechny nevyžádané funkcionality, např. IPv6, autorun a LanMan.

ZAMEZTE PŘÍMÉMU PŘÍSTUPU PRACOVNÍCH STANIC NA INTERNET
a směrujte provoz přes split DNS server, e-mailový server nebo autentizovaný web proxy server. Nezapomeňte vynutit pro IPv4 i IPv6.

UŽIVATELÉ

ZAVEĎTE CENTRÁLNÍ SPRÁVU UŽIVATELSKÝCH ÚČTŮ A OPRÁVNĚNÍ
a nastavte jednotnou bezpečnostní politiku. Účtům, u kterých to není vyžadováno, odeberte rozšířená oprávnění a zakažte spouštění skriptů, instalaci softwaru, úpravy registru atd.

VYNUCUJTE VÍCEFAKTOROVOU AUTENTIZACI
zejména pro akce vyžadující vyšší úroveň oprávnění a kritické operace jako vzdálený přístup nebo přístup k citlivým informacím.

ODDĚLTE ADMINISTRÁTORSKÉ ÚČTY OD BĚŽNÝCH
Pro správu používejte speciální účet pro administraci systémů. Pro své ostatní pracovní aktivity (e-mail, web atd.) používejte běžný neprivilegovaný účet.

PŘIDĚLTE KAŽDÉMU SPRÁVCI VLASTNÍ ÚČET PRO ADMINISTRACI SYSTÉMŮ
Nepoužívejte sdílené účty.

ZABEZPEČTE LOKÁLNÍ ADMINISTRÁTORSKÉ ÚČTY
a nastavte unikátní heslo na každé stanici. V prostředí Windows můžete využít například LAPS (Local Administrator Password Solution).

VYNUŤTE POUŽÍVÁNÍ SILNÝCH HESEL
s ohledem na vyžadovanou složitost, délku a dobu platnosti. Zamezte opakovanému použití stejných hesel a používání slovníkových výrazů. Vynutte změnu hesla, existuje-li podezření, že bylo kompromitováno.

PRAVIDELNĚ KONTROLUJTE UŽIVATELSKÉ ÚČTY A JEJICH OPRÁVNĚNÍ
a to jak lokální, tak centrálně spravované.

www.nukib.cz

Národní úřad pro kybernetickou a informační bezpečnost

BEZPEČNOSTNÍ DOPORUČENÍ PRO ADMINISTRÁTORY

Zaměřeno na:

- infrastrukturu,
- stanice & servery,
- uživatele.

Dvě formy:

- plakát,
- brožura.

více na adrese:

https://osveta.nukib.cz/