Nová éra kybernetické bezpečnosti

IcyBear. Bezpečnostní řešení, které myslí za Vás!

IcyBear Czech Republic s.r.o.

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

EA-1. Motivace	Zabezpečená firma	Soulad s předpisy, se zákony a s regulatorními rámci - GDPR, NIS2, ZoKB	Hodnota dat a aktiv	Bezpečnostní doporučení NÚKIB	
EA-2. Strategie	Strategie bezpečnosti	Plán kontinuity podnikání (BCP)	Strategie kybernetické odolnosti		
EA-3. Operativa	Zabezpečené procesy	IAM - Správa identit a přístupových práv	SIEM - Správ bezpečnostních incidentů	Řízení bezpečnostních rizik	Zabezpečení dodavatelského řetězce
EA-4. Informace	Zabezpečené informace	ISO 27001 - Systém řízení bezpečnosti informací			
EA-5. Aplikace	Zabezpečené aplikace	CSaaS: Outsourcované bezpečnostní služby	SOC 24/7: Centralizované monitorování a reakce na bezpečnostní incidenty	DevSecOps: Integrace bezpečnosti do vývojového cyklu	
EA-6. Data	Zabezpečená data	CASB - Zabezpečení dat v cloudových službách			
EA-7. Sítě	Zabezpečené sítě	Architektura nulové důvěry	NGFW - Pokročilá ochrana perimetru	IoT Bezpečnost	VPN
EA-8. Aktiva	Zabezpečená aktiva	Bezpečnost koncových bodů	Evidence a správa aktiv		

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

ICYBEAR

Vybrané organizace a firmy

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

Vybrané organizace a firmy

Velké organizace, firmy, města a ministerstva

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

Vybrané organizace a firmy

Velké organizace, firmy, města a ministerstva

Jednotlivci, malé a střední organizace, firmy a obce

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

Vybrané organizace a firmy

Velké organizace, firmy, města a ministerstva

Jednotlivci, malé a střední organizace, firmy a obce

ICYBEAR
CYBER SECURITY

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

- Díky AI jsou kybernetickými útoky ohrožení i jednotlivci a malé organizace.

Jednotlivci,
malé a střední
organizace,
firmy a obce

ICYBEAR
CYBER SECURITY

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

- Díky AI jsou kybernetickými útoky ohrožení i jednotlivci a malé organizace.
- Jak si mohou dovolit pořídit si stejně kvalitní zabezpečení svých aktiv?

Jednotlivci, malé a střední organizace, firmy a obce

ICYBEAR
CYBER SECURITY

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

- Díky AI jsou kybernetickými útoky ohrožení i jednotlivci a malé organizace.
- Jak si mohou dovolit pořídit si stejně kvalitní zabezpečení svých aktiv?
- Evoluce jim jde naproti a díky SaaS cenově zpřístupňuje tyto služby i jim.

Jednotlivci, malé a střední organizace, firmy a obce

ICYBEAR
CYBER SECURITY

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

- Díky AI jsou kybernetickými útoky ohrožení i jednotlivci a malé organizace.
- Jak si mohou dovolit pořídit si stejně kvalitní zabezpečení svých aktiv?
- Evoluce jim jde naproti a díky SaaS cenově zpřístupňuje tyto služby i jim.

Jednotlivci, malé a střední organizace, firmy a obce

od 3.600Kč/ 1 uživatele/ 1 rok !!!

ICYBEAR
CYBER SECURITY

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

Jednotlivci,
malé a střední
organizace,
firmy a obce

ICYBEAR
CYBER SECURITY

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

ICYBEAR

GARANCE VYPLACENÍ PENĚZ

ZA VŠECHNY PŘÍPADNÉ VZNIKLÉ ŠKODY!!!

Jednotlivci,
malé a střední
organizace,
firmy a obce

ICYBEAR
CYBER SECURITY

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

Partnerem ICY BEAR, doplňujícím komplexní řešení pro kybernetickou bezpečnost malých a středních organizací, je společnost Com-Sys TRADE spol. s.r.o., která úspěšně působí na českém trhu informačních a komunikačních technologií již od roku 1990.

Zaměřuje se na komplexní dodávky v tomto oboru, tedy analýzu, návrh, realizaci a servis projektů provozní, datové a komunikační infrastruktury společností a organizací se zaměřením na služby správy, managementu, servicedesku a helpdesku.

V jejich projektech přebírají kompletní garanci za navržené parametry, funkčnost, údržbu a rozvoj realizovaného systému.

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

EA-1. Motivace	Zabezpečená firma	Soulad s předpisy, se zákony a s regulatorními rámci - GDPR, NIS2, ZoKB	Hodnota dat a aktiv	Bezpečnostní doporučení NÚKIB	
EA-2. Strategie	Strategie bezpečnosti	Plán kontinuity podnikání (BCP)	Strategie kybernetické odolnosti		
EA-3. Operativa	Zabezpečené procesy	IAM - Správa identit a přístupových práv	SIEM - Správ bezpečnostních incidentů	Řízení bezpečnostních rizik	Zabezpečení dodavatelského řetězce
EA-4. Informace	Zabezpečené informace	ISO 27001 - Systém řízení bezpečnosti informací			
EA-5. Aplikace	Zabezpečené aplikace	CSaaS: Outsourcované bezpečnostní služby	SOC 24/7: Centralizované monitorování a reakce na bezpečnostní incidenty	DevSecOps: Integrace bezpečnosti do vývojového cyklu	
EA-6. Data	Zabezpečená data	CASB - Zabezpečení dat v cloudových službách			
EA-7. Sítě	Zabezpečené sítě	Architektura nulové důvěry	NGFW - Pokročilá ochrana perimetru	IoT Bezpečnost	VPN
EA-8. Aktiva	Zabezpečená aktiva	Bezpečnost koncových bodů	Evidence a správa aktiv		

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

Firemní architektura a kybernetická bezpečnost jsou úzce propojené oblasti. Firemní architektura poskytuje komplexní pohled na celou organizaci. Tento holistický přehled je zásadní pro efektivní implementaci kybernetické bezpečnosti:

1. Zakomponováním bezpečnosti do podnikové architektury umožňuje lépe identifikovat klíčová aktiva a kritické systémy společnosti, které vyžadují zvýšenou ochranu.

2. Podniková architektura pomáhá lépe mapovat datové toky napříč organizací, což je nezbytné pro správné nastavení bezpečnostních kontrol.

3. Architektonický přístup zajišťuje, že bezpečnostní požadavky jsou zohledněny již v počátečních fázích návrhu a vývoje systémů. Což je mnohem efektivnější než jejich dodatečná implementace.

4. Přímá integrace bezpečnosti do podnikové architektury umožňuje konzistentní přístup k řízení rizik napříč celou organizací.

5. A další výhody...

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

ICYBEAR

EA8: Aktiva

Definování stupně důležitosti hmotných a nehmotných aktiv - a poté zabezpečení!

Endpoint Security - ochrana koncových zařízení. Řešení Endpoint Detection and Response (EDR).

- **Firewall -** Osobní firewall, který blokuje neautorizovaný síťový provoz, který by mohl ohrozit zařízení.
- **Šifrování -** Ochrana citlivých dat na koncových bodech šifrováním, což znamená, že data jsou k dispozici pouze oprávněným uživatelům, i když jsou zařízení ukradena nebo ztracena.
- **Správa identit a přístupu (IAM) -** Ověření a správa přístupových práv uživatelů k citlivým datům a systémům, aby se zajistilo, že pouze oprávnění uživatelé mohou přistupovat k určitým informacím.
- **Bezpečnostní patchování a aktualizace:** Pravidelná aktualizace softwaru a operačních systémů na koncových bodech, aby se odstranily zranitelnosti, které by mohly být využity k útokům.
- **Detekce a prevence průniků (IDS/IPS):** Systémy pro detekci a prevenci útoků, které monitorují aktivitu na koncových bodech a reagují na podezřelé chování nebo pokusy o útok.
- **Bezpečnostní politiky a správa zařízení:** Zajištění, že zařízení jsou správně konfigurována a chráněna podle organizace stanovených bezpečnostních politik, včetně blokování neoprávněného připojení zařízení nebo instalace neautorizovaných aplikací.

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

ICYBEAR

EA-1. Motivace

EA-2. Strategie

EA-3. Operativa

EA-4. Informace

EA-5. Aplikace

EA-6. Data

EA-7. Sítě

EA-8. Aktiva

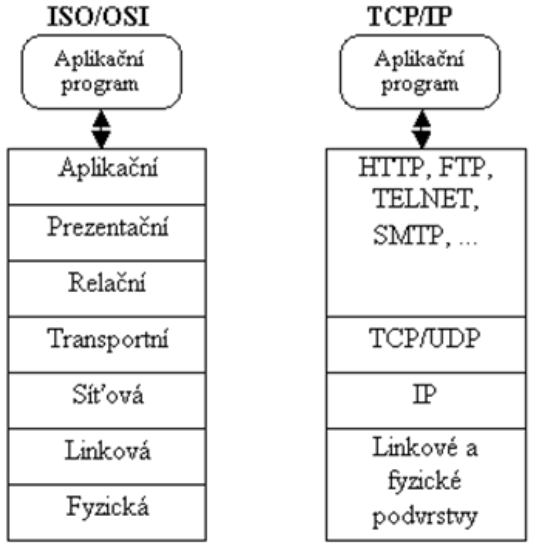
EA7: Síťová vrstva

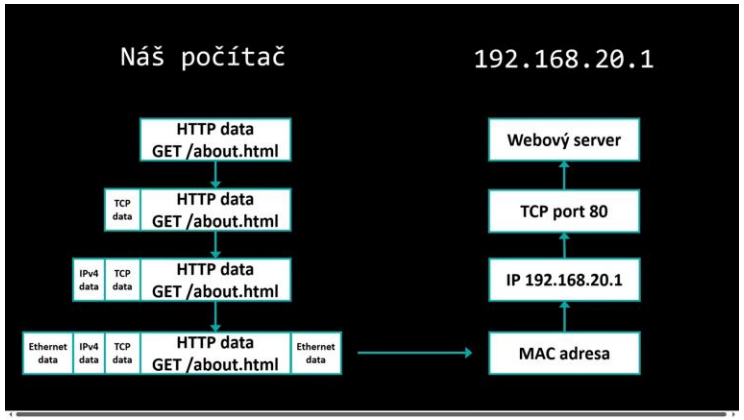
Definování stupně důležitosti komunikačních sítí - a poté zabezpečení!

- **VPN -** Technologie, která umožňuje bezpečné a šifrované připojení mezi vaším zařízením (například počítačem, telefonem nebo tabletem) a vzdálenou sítí, obvykle internetem.
- **Zabezpečení úložišť a cloudových architektur** - ochrana dat uložených v cloudu
- **Segmentace sítě** - Rozdělení sítě na izolované části
- **Next-gen firewally** - Pokročilá ochrana perimetru. Pokročilý firewall systém (nebo Next-Generation Firewall – NGFW) představuje moderní typ firewallu, který jde nad rámec tradičních firewallů a nabízí širší spektrum funkcí pro ochranu sítě. Tento typ firewallu je navržen tak, aby poskytoval nejen kontrolu síťového provozu, ale i pokročilou detekci hrozeb a prevenci, čímž zajišťuje komplexní bezpečnostní ochranu.
- **Produkty detekce a reakce na síť (NDR)** - Detekují abnormální chování systému aplikováním behaviorální analýzy na data síťového provozu. Nepřetržitě analyzují síťové pakety nebo metadata provozu uvnitř interních sítí (východ-západ) a mezi interními a externími sítěmi (sever-jih).
- **Kryptografické algoritmy -** NÚKIB definuje minimální požadavky pro kryptografické algoritmy
- **Informační toky a bezpečnostní zóny** - řízení přenosu informací mezi systémy

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti





Rozdělení serverů podle jednotlivých vrstev OSI modelu:

Aplikační vrstva:
Webový server (HTTP/HTTPS); Databázový server; Souborový server; E-mailový server (SMTP, POP3, IMAP); Aplikační server; DNS server; Většina proxy serverů; FTP server; Herní server; VPN server; Virtualizační server; Print server; SSH server; NTP server; LDAP server; Media server; Terminal server; Radius server; Backup server; Monitoring server; IDS/IPS server; TFTP server; IRC server; Cache server; Kerberos server

Transportní vrstva:
- Load balancer (rozděluje TCP spojení)
- Některé typy proxy serverů (pracující na úrovni TCP)

Síťová vrstva:
- DHCP server (pracuje s IP adresami)
- Routing servery (směrování IP paketů)

Linková vrstva:
- Některé typy switchů s pokročilými funkcemi serveru
- Některé typy firewall serverů fungující na linkové vrstvě

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

ICYBEAR

EA6: Datová vrstva

Definování stupně důležitosti dat - a poté jejich zabezpečení!

- **Šifrování (Encryption)** - Chrání data před neoprávněným čtením.
- **Kontrola přístupu (Access Control)** - Umožňuje přístup k datům pouze oprávněným osobám.
- **Zálohování a obnova (Backup & Recovery)** - Ochrana proti ztrátě nebo poškození dat (např. ransomwarem).
- **Detekce úniku dat (Data Loss Prevention/ DLP)** - Zabraňuje nechtěnému nebo škodlivému odesílání citlivých dat mimo organizaci.
- **Audit a monitorování přístupu k datům** - Zaznamenávání a vyhodnocování toho, kdo data používá, kdy a jak.
- **Klasifikace a označování dat (Data Classification & Tagging)** - Rozlišení úrovně citlivosti dat (např. veřejné / interní / důvěrné / tajné).
- **Maskování a anonymizace dat** - Ochrana osobních a citlivých údajů při testování, analýze nebo sdílení.
- **Zajištění integrity dat** - Ověření, že data nebyla neoprávněně změněna.
- **Správa životního cyklu dat** - Pravidla pro uchovávání, archivaci a bezpečné mazání dat.

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

ICYBEAR

EA5: Aplikační vrstva

Definování stupně důležitosti aplikací a informačních systémů - a poté jejich zabezpečení!

- **CSaaS (Cybersecurity as a Service)** je model poskytování bezpečnostních služeb prostřednictvím cloudu. V tomto modelu externí poskytovatelé nabízí různé bezpečnostní řešení, jako je ochrana před kybernetickými útoky, detekce hrozeb, šifrování, autentifikace a další bezpečnostní služby, které jsou poskytovány jako služba na bázi cloudu.
- **SOC 24/7 (Security Operations Center)** je bezpečnostní centrum, které funguje nepřetržitě 24 hodin denně, 7 dní v týdnu, s cílem monitorovat, detekovat a reagovat na kybernetické hrozby a incidenty v reálném čase. Tento typ centra je klíčový pro ochranu organizací před bezpečnostními riziky, jako jsou hackeři, malware, phishing a další kybernetické útoky.
- **DevSecOps** je zkratkami pro vývoj, zabezpečení a provoz. Jde o nezbytný proces při vytváření nových programů, který vede k vyššímu zabezpečení jejich softwaru. Díky DevSecOps dochází k optimalizaci nákladů na dodržování bezpečnostních předpisů a zrychlování vývoje software.

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

ICYBEAR

EA4: Informační vrstva

Definování stupně důležitosti informací a znalostí – a poté jejich zabezpečení!

Informační bezpečnost je širší koncept než je kybernetická bezpečnost. Zabývá ochranou informací v podobě (digitální a fyzické - papírové dokumenty atd.). Zaměřuje se na zachování důvěrnosti, integrity a dostupnosti informací bez ohledu na jejich formu nebo způsob uložení.

- **Rozsah:** Pokrývá veškeré informace včetně papírových dokumentů, ústního předávání informací, fyzického zabezpečení atd.
- **Cíle:** Ochrana všech informačních aktivních organizací.
- **Hrozby:** Řeší širší spektrum hrozeb včetně přírodních katastrof, lidských chyb, krádeží.
- **Nástroje a postupy:** Zahrnuje i fyzické kontroly, školení personálu, správu dokumentů.

ISO 27001 - Systém řízení bezpečnosti informací

- Účinnost od roku 2005.

- Vztahuje se na všechny organizace, které chtějí chránit svá aktiva.

- Hlavní povinnosti: Zavedení opatření na zajištění bezpečnosti informací. Certifikace.

- Řízení aktiv a rizik. Řízení kontinuity činností. Incident management

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

ICYBEAR

EA-1. Motivace

EA-2. Strategie

EA-3. Operativa

EA-4. Informace

EA-5. Aplikace

EA-6. Data

EA-7. Sítě

EA-8. Aktiva

EA3: Business vrstva

Definování stupně důležitosti procesů a zaměstnanců společnosti - a poté jejich zabezpečení!

Vrcholový management se aktivně podílí na řízení kyberbezpečnosti! Manažer kybernetické bezpečnosti je zodpovědný za nastavení systému řízení bezpečnosti informací, především za určení aktiv a jejich zranitelnosti, nastavení bezpečnostních opatření, řízení rizik a jejich kontrolu.

- **SIEM (Security Information and Event Management)** - centralizovaná analýza bezpečnostních událostí
- **IAM (Identity and Access Management)** - správa identit a přístupových oprávnění
- **Bezpečnostní politiky a procedury** - dokumentované zásady a postupy
- **Incident Response Plan** - formalizovaný postup reakce na bezpečnostní incidenty
- **Bezpečnostní role a zodpovědnosti** - jasné definování kompetencí v oblasti bezpečnosti
- **Řízení dodavatelů a třetích stran** - bezpečnostní požadavky na externí entity
- **Program řízení rizik** - systematická identifikace, analýza a zmírňování bezpečnostních rizik

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

ICYBEAR

EA-1. Motivace

EA-2. Strategie

EA-3. Operativa

EA-4. Informace

EA-5. Aplikace

EA-6. Data

EA-7. Sítě

EA-8. Aktiva

EA2: Strategická vrstva

Navržení postupů implementace kybernetické bezpečnosti. Řízení bezpečnostní politiky a dokumentace.

Zero trust principy v bezpečnostní architektuře organizace.

- **Bezpečnostní strategie** - dlouhodobá vize a směřování kybernetické bezpečnosti
- **Bezpečnostní politiky a směrnice** - formální dokumenty definující pravidla a postupy pro zabezpečení informací
- **Governance framework** - struktura řízení bezpečnosti v organizaci
- **Bezpečnostní architektura** - celkový návrh bezpečnostního prostředí
- **Bezpečnostní metriky** - strategické ukazatele pro hodnocení úrovně zabezpečení
- **Investiční strategie** - plánování zdrojů pro bezpečnostní iniciativy
- **Plán kontinuity podnikání (BCP)** - strategie pro zachování funkcí při narušení
- **Plán obnovy po havárii (DRP)** - strategie obnovení systémů po bezpečnostním incidentu

ISO 27001: účinnost d roku 2005 (poslední verze standardu je z roku 2022).

- Vztahuje se na všechny organizace, které chtějí chránit svá aktiva.
- Hlavní povinnosti: Zavedení opatření na zajištění bezpečnosti informací (certifikace).
- Řízení aktiv a rizik. Řízení kontinuity činností. Incident management.

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

ICYBEAR

EA-1. Motivace

EA-2. Strategie

EA-3. Operativa

EA-4. Informace

EA-5. Aplikace

EA-6. Data

EA-7. Sítě

EA-8. Aktiva

EA1: Motivační vrstva

Spolehlivost ochrany osobních a citlivých údajů se následně projeví v dobrém vnímání organizace ze strany veřejnosti a klientů.

- **Compliance a regulatorní rámce** - identifikace a dodržování zákonných požadavků (GDPR, NIS2, ZoKB)
- **Hodnota aktiv** - kategorizace aktiv podle jejich důležitosti pro organizaci
- **Bezpečnostní povědomí** - motivace zaměstnanců k bezpečnému chování
- **Kybernetická odolnost** - motivace k vytvoření systémů schopných odolávat a zotavit se z útoků

Soulad s NIS2, která výrazně rozšiřuje oblast působnosti platné legislativy a představuje nové řešení pro posílení a zabezpečení evropského kyberprostoru. 50 a více zaměstnanců, ročním obratem více než 10 milionů euro. kritická infrastruktura (KI)

Soulad se zákonem o kybernetické bezpečnosti – účinnost od roku 2025:

Vztahuje se na: Poskytovatele regulované služby. Hlavní povinnosti: Určení regulované služby samoidentifikace a registrace prostřednictvím portálu NÚKIB. Zavedení opatření na zajištění kybernetické bezpečnosti (v režimu vyšších, nebo nižších povinností).

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

Ochrana firemních aktiv pomocí pokročilého bezpečnostního řešení IcyBear:

Zero - Day ochrana v pokročilém bezpečnostním řešení IcyBear.

Zero-Day ochrana se týká opatření a technologií, které chrání systémy a aplikace před zranitelnostmi, které jsou neznámé nebo dosud neopravené, tedy před útoky, které využívají zero-day (zero-day vulnerability) zranitelnosti.

- Behaviorální analýza: Monitorování chování aplikací a systémů v reálném čase.
- Antivirový a antimalwarový software s heuristickou analýzou: Tento software se snaží detekovat neznámý malware na základě vzorců chování.
- Intrusion Prevention Systems (IPS): Tato zařízení a systémy sledují síťovou komunikaci a hledají podezřelé aktivity nebo útoky.
- Sandboxing: Technologie, která spouští aplikace nebo kód v izolovaném prostředí (sandbox), aby zjistila, zda má škodlivý charakter.
- Patch management: Správa aktualizací a jejich včasné nasazování může minimalizovat riziko útoků, které využívají zranitelnosti, které se ještě neobjevily.
- Threat Intelligence: Aktivní sledování a analýza hrozeb, včetně výzkumu nových zranitelností a útoků.
- A další…

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

Ochrana firemních aktiv pomocí pokročilého bezpečnostního řešení IcyBear:

Popis vrstev pokročilého bezpečnostního řešení IcyBear:

- Nejlepší podniková bezpečnostní řešení softwaru fungují ve více vrstvách. Jen tak vytvářejí solidní obranu proti kybernetickým hrozbám.
- Každá vrstva přináší konkrétní výhodu – od detekce a prevence pokročilých hrozeb po ochranu dat na koncových zařízeních.
- Společně vytvářejí robustní bezpečnostní systém, který jde daleko za rámec standardních antivirů.
- Dává uživatelům klid a jistotu, že jejich zařízení, data i komunikace jsou v bezpečí před moderními kybernetickými útoky.

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

ICYBEAR

EA-1. Motivace

EA-2. Strategie

EA-3. Operativa

EA-4. Informace

EA-5. Aplikace

EA-6. Data

EA-7. Sítě

EA-8. Aktiva

I. Ochrana koncových zařízení (Endpoint Protection):

1. Antimalware s vícevrstvou detekcí:

Kombinuje signatury, heuristiku a strojové učení pro ochranu před známým i neznámým malwarem.

Běžný antivir: Používá signatury. Naše výhoda: Detekce neznámých hrozeb pomocí strojového učení.

Antimalware je typ bezpečnostního softwaru, který je navržen k detekci, prevenci a odstranění škodlivého softwaru (malwaru) z počítačových systémů. Mezi běžné typy malwaru, které antimalware programy vyhledávají, patří viry, trojské koně, spyware, ransomware, adware a červi.

2. Behaviorální analýza v reálném čase:

Aktivně sleduje podezřelé chování procesů a zastavuje útoky, než napáchají škody.

Běžný antivir: Základní sledování aktivit. Naše výhoda: Pokročilé analýzy chování s AI.

Behaviorální analýza - Monitorování chování aplikací a systémů v reálném čase. Pokud program nebo aplikace vykazuje podezřelé nebo neobvyklé chování, může být okamžitě zablokován, což pomáhá detekovat útoky i bez znalosti konkrétní zranitelnosti.

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

I. Ochrana koncových zařízení (Endpoint Protection):

3. Pokročilý Anti-Exploit s cílenou prevencí:
Zamezuje útokům na zranitelnosti ve vašich aplikacích (např. prohlížečích, Office).

Běžný antivir: Tuto funkci většinou nemá. Naše výhoda: Prevence exploitů i na zero-day zranitelnosti.

Anti-Exploit je bezpečnostní program, který poskytuje další vrstvu ochrany tím, že detekuje a blokuje exploity a zranitelnosti, které antivirový software nemusí odhalit.

4. HyperDetect (AI-driven):
Chrání díky umělé inteligenci, která předvídá a blokuje nové hrozby dříve, než se spustí.

Běžný antivir: Chybí. Naše výhoda: Prediktivní ochrana.

Výhodou AI-driven řešení jako HyperDetect je schopnost adaptace na nové typy útoků bez nutnosti čekat na aktualizace databáze signatur, což zvyšuje ochranu proti tzv. "zero-day" útokům (útokům využívajícím dosud neznámé zranitelnosti).

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

ICYBEAR

I. Ochrana koncových zařízení (Endpoint Protection):

5. Ransomware Mitigation s obnovou dat:
Zastaví ransomware a automaticky obnoví soubory, které by jinak byly zašifrované.

Běžný antivir: Blokuje ransomware, ale neobnoví data. Naše výhoda: Plná obnova dat.

Ransomware Mitigation s obnovou dat je komplexní bezpečnostní řešení zaměřené na ochranu proti ransomwaru a schopnost obnovit data v případě úspěšného útoku. Ransomware je typ škodlivého softwaru, který zašifruje data uživatele nebo organizace a následně požaduje výkupné (ransom) za poskytnutí dešifrovacího klíče. Ransomware Mitigation s obnovou dat kombinuje preventivní opatření s možností obnovy, aby minimalizoval dopady těchto útoků.

6. Ochrana proti keyloggerům s blokováním přístupu:
Zabraňuje odposlechu vašich hesel a citlivých údajů při psaní.

Běžný antivir: Detekuje pouze známé keyloggery. Naše výhoda: Chrání i proti novým metodám odposlechu.

Ochrana proti keyloggerům s blokováním přístupu je specializované bezpečnostní řešení, které se zaměřuje na prevenci a blokování keyloggerů – škodlivého softwaru, který zaznamenává stisknuté klávesy uživatele s cílem ukrást citlivé informace jako hesla, přihlašovací údaje nebo osobní data.

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

ICYBEAR

EA-1. Motivace

EA-2. Strategie

EA-3. Operativa

EA-4. Informace

EA-5. Aplikace

EA-6. Data

EA-7. Sítě

EA-8. Aktiva

I. Ochrana koncových zařízení (Endpoint Protection):

7. Detekce phishingu s dynamickou URL analýzou:
Blokuje falešné stránky a e-maily dříve, než na ně kliknete.

Běžný antivir: Detekuje pouze známé stránky. Naše výhoda: Reálná analýza odkazů v reálném čase.

Detekce phishingu s dynamickou URL analýzou je pokročilá bezpečnostní technologie, která pomáhá identifikovat a blokovat phishingové útoky prostřednictvím komplexní analýzy webových adres v reálném čase. Tato technologie je obzvláště cenná, protože phishingové stránky jsou často krátkodobé a rychle se mění, aby se vyhnuly detekci. Dynamická URL analýza dokáže identifikovat i nové phishingové stránky, které ještě nebyly zařazeny do databází nebezpečných stránek.

8. Pokročilé řízení aplikací (Application Control):
Umožňuje spouštět pouze ověřené aplikace, což minimalizuje riziko infekce.

Běžný antivir: Chybí. Naše výhoda: Detailní kontrola podle firemních pravidel.

Pokročilé řízení aplikací (Application Control) je komplexní bezpečnostní technologie, která umožňuje organizacím a uživatelům přesně určit, které aplikace mohou být spuštěny v jejich systémech, čímž výrazně snižují riziko škodlivého softwaru a neoprávněných programů.

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

ICYBEAR

I. Ochrana koncových zařízení (Endpoint Protection):

9. Kontrola zařízení (Device Control):
Omezuje přístup externích zařízení, jako jsou USB, a chrání před jejich zneužitím.

Běžný antivir: Omezená kontrola USB zařízení. Naše výhoda: Komplexní správa zařízení.

Kontrola zařízení (Device Control) je bezpečnostní technologie, která umožňuje organizacím řídit a monitorovat používání externích a periferních zařízení připojených k firemním počítačům a síti. Tato technologie pomáhá předcházet úniku dat, zavlečení malwaru a neautorizovanému přístupu prostřednictvím hardwarových zařízení.

10. Web filtering s pokročilou kategorizací:
Zamezuje přístupu na škodlivé weby pomocí analýzy v reálném čase.

Běžný antivir: Omezená funkce. Naše výhoda: Dynamická kategorizace webů pomocí AI.

Web filtering s pokročilou kategorizací je komplexní bezpečnostní řešení, které umožňuje organizacím a uživatelům řídit přístup k webovému obsahu na základě sofistikovaného kategorizačního systému.
Tato technologie jde daleko za jednoduché blokování konkrétních URL adres a nabízí mnohem pokročilejší možnosti řízení internetového přístupu.

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

ICYBEAR

I. Ochrana koncových zařízení (Endpoint Protection):

11. Ochrana proti brute force útokům:
Zablokuje pokusy o prolomení hesla opakovanými pokusy.

Běžný antivir: Chybí. Naše výhoda: Prevence přímých útoků na přihlašování.

Ochrana proti brute force útokům je bezpečnostní mechanismus navržený k detekci, prevenci a blokování pokusů o neoprávněný přístup prostřednictvím systematického zkoušení různých kombinací hesel nebo přihlašovacích údajů. Tyto útoky se spoléhají na hrubou výpočetní sílu a opakované pokusy, dokud není nalezena správná kombinace.

12. Ochrana webových kamer:
Zabrání neoprávněnému přístupu k vaší webové kameře.

Běžný antivir: Dostupné jen v některých řešeních. Naše výhoda: Integrovaná ochrana webkamery i mikrofonu.

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

ICYBEAR

I. Ochrana koncových zařízení (Endpoint Protection):

13. Detekce škodlivého síťového provozu (Network-based Threat Detection):
Monitoruje a blokuje podezřelý provoz v síti.

Běžný antivir: Chybí. Naše výhoda: Identifikace nových síťových útoků.

Detekce škodlivého síťového provozu (Network-based Threat Detection) je pokročilá bezpečnostní technologie, která monitoruje a analyzuje veškerý síťový provoz s cílem identifikovat a blokovat podezřelé nebo škodlivé aktivity. Tato technologie tvoří kritickou část komplexní bezpečnostní strategie, která dokáže odhalit hrozby, které by mohly uniknout tradičním zabezpečením na úrovni koncových bodů.

14. Blokace škodlivého makro kódu v dokumentech:
Zastaví hrozby skryté v Office dokumentech, než spustí škodlivý kód.

Běžný antivir: Detekuje jen známé makra. Naše výhoda: Analýza neznámých skriptů.

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

ICYBEAR

EA-1. Motivace

EA-2. Strategie

EA-3. Operativa

EA-4. Informace

EA-5. Aplikace

EA-6. Data

EA-7. Sítě

EA-8. Aktiva

II. Ochrana mobilních zařízení (Mobile Protection):

15. Harmony Mobile Threat Defense: Komplexní ochrana vašeho telefonu proti zranitelnostem, škodlivým aplikacím a síťovým útokům.

16. Zabezpečení VPN připojení: Chrání vaši komunikaci ve veřejných sítích pomocí šifrovaného připojení.

17. Phishing ochrana pro mobilní zařízení: Blokuje podvodné odkazy a SMS ještě předtím, než jim naletíte.

18. Detekce nebezpečných mobilních aplikací: Zamezí instalaci škodlivých aplikací, které mohou ohrozit vaše data.

19. Ochrana proti útokům typu MITM (Man-in-the-Middle): Detekuje a zastavuje pokusy o odposlech vaší komunikace.

20. Harmony Mobile Root/Jailbreak Detection: Upozorní vás na pokusy o neoprávněné zásahy do systému telefonu.

21. Ochrana proti nebezpečným mobilním sítím (Wi-Fi Threat Detection): Chrání vás před připojením k podvodným Wi-Fi sítím.

Mobilní ochrana většinou není součástí běžných antivirů, takže všechny funkce zde jsou pokročilé výhody.

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

III. Správa oprav (Patch Management):

22. Automatická prioritizace bezpečnostních oprav: Opravuje zranitelnosti v systému, než je hackeři stihnou zneužít

23. Správa aktualizací třetích stran: Udržuje aplikace jako Adobe, Java nebo Zoom aktuální a bezpečné.

24. Vulnerability Assessment (analýza zranitelností): Analyzuje slabá místa a navrhuje, co opravit nejdříve.

25. Dynamická detekce starých verzí softwaru: Upozorní na aplikace, které už nejsou podporované a mohou být zranitelné.

Běžné antiviry zde nemají žádné funkce – jedná se o jednoznačnou výhodu pokročilých řešení.

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

ICYBEAR

EA-1. Motivace

EA-2. Strategie

EA-3. Operativa

EA-4. Informace

EA-5. Aplikace

EA-6. Data

EA-7. Sítě

EA-8. Aktiva

IV. Šifrování a ochrana dat (Data Protection):

26. Šifrování na úrovni aplikací: Chrání citlivé dokumenty a e-maily ještě před odesláním.

27. Prevence úniku dat (DLP): Zabrání neoprávněnému přenosu důvěrných informací ven z firmy.

28. Zabezpečení cloudových dat: Monitoruje vaše soubory v cloudu a blokuje podezřelé aktivity.

29. Správa šifrovacích klíčů: Zajišťuje bezpečné uchování vašich šifrovacích klíčů.

30. Zálohování a obnova dat po útoku: Pravidelné zálohy, které minimalizují dopad ransomware útoků.

31. Šifrování výměny dat přes USB: Chrání přenos dat na externích zařízeních šifrováním.

Běžné antiviry většinou šifrování ani správu dat neřeší.

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

V. Ochrana e-mailové komunikace (Email Security):

32. Antispam: Filtruje nevyžádanou poštu a snižuje riziko infekce.

33. Blokování škodlivých příloh s dynamickou analýzou: Analýza příloh v sandboxu detekuje i dosud neznámé hrozby.

34. Analýza spear phishingu (cílené útoky): Identifikuje pokusy o podvod zaměřené na vás nebo vaši organizaci.

35. Pokročilá URL analýza v reálném čase: Blokuje odkazy směřující na škodlivé stránky.

36. Prevence e-mailového spoofingu (Anti-Spoofing): Chrání vás před falešnými e-maily, které napodobují legitimní odesílatele.

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

EA-1. Motivace

EA-2. Strategie

EA-3. Operativa

EA-4. Informace

EA-5. Aplikace

EA-6. Data

EA-7. Sítě

EA-8. Aktiva

VI. Detekce a reakce na hrozby (Threat Detection and Response):

37. Endpoint Detection and Response (EDR): Sleduje aktivitu zařízení a reaguje na hrozby v reálném čase.

38. Threat Hunting (proaktivní detekce): Vyhledává potenciální hrozby ještě předtím, než zaútočí.

39. Forenzní analýza po incidentu: Umožňuje pochopit, co přesně se stalo, a předejít dalším útokům.

40. Automatizovaná reakce na incidenty: Automaticky izoluje infikované zařízení a zastaví šíření hrozby.

41. Detekce fileless útoků (Memory-based Attack Prevention): Chrání před útoky, které probíhají přímo v operační paměti.

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

VII. Pokročilé funkce (Advanced Tools):

42. Machine Learning Threat Prevention: Prediktivní ochrana založená na analýze chování hrozeb pomocí umělé inteligence.

V této sekci běžné antiviry nemají ani EDR, ani forenzní analýzu.

Pokročilé bezpečnostní řešení IcyBear - Souhrn:

- Každá vrstva přináší konkrétní výhodu – od detekce a prevence pokročilých hrozeb po ochranu dat na koncových zařízeních.
- Společně vytvářejí robustní bezpečnostní systém, který jde daleko za rámec standardních antivirů.
- Dává uživatelům klid a jistotu, že jejich zařízení, data i komunikace jsou v bezpečí před moderními kybernetickými útoky.

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

ICYBEAR

EA-1. Motivace

EA-2. Strategie

EA-3. Operativa

EA-4. Informace

EA-5. Aplikace

EA-6. Data

EA-7. Sítě

EA-8. Aktiva

JEDNODENNÍ INTENZIVNÍ ANALÝZA BEZPEČNOSTI – RISKRECON ASSAULT – POPIS SLUŽBY (1/3)

RiskRecon Assault je unikátní služba zaměřená na rychlou a efektivní analýzu bezpečnosti vaší IT infrastruktury.

Během jednodenní návštěvy našeho konzultanta se zaměříme na následující klíčové aspekty:

- Prověření 7 klíčových typů útoků na uživatele.
- Testování síly zabezpečení aktuálního antivirového softwaru prostřednictvím simulace ransomware útoku.
- Ověření možnosti ovládnutí počítače a testování detekce odesílání dat mimo společnost.
- Kontrola nastavení perimetrového firewallu.
- Analýza zabezpečení interních sítí a připojených zařízení včetně mobilních zařízení a vzdáleného přístupu.
- Hodnocení efektivity aktuálních bezpečnostních protokolů a procedur.
- Prověření odolnosti proti sociálnímu inženýrství a phishingovým útokům

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

JEDNODENNÍ INTENZIVNÍ ANALÝZA BEZPEČNOSTI – RISKRECON ASSAULT – POPIS SLUŽBY (2/3)

Konzultant projde s majitelem nebo IT manažerem klíčové služby, posoudí potenciální dopady na firmu a sestaví seznam největších rizik.

Tento proces zahrnuje ocenění dopadů identifikovaných rizik na operace a finanční zdraví firmy.

Výstupem služby bude podrobný report, který zahrnuje:

- Souhrn zjištění a hodnocení aktuálního stavu bezpečnosti.

- Doporučení pro zlepšení a konkrétní kroky pro implementaci těchto změn.

Služba RiskRecon Assault je ideální pro firmy, které hledají rychlý a důkladný přehled o svém bezpečnostním stavu, a chtějí efektivně reagovat na potenciální hrozby.

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

ICYBEAR

EA-1. Motivace

EA-2. Strategie

EA-3. Operativa

EA-4. Informace

EA-5. Aplikace

EA-6. Data

EA-7. Sítě

EA-8. Aktiva

JEDNODENNÍ INTENZIVNÍ ANALÝZA BEZPEČNOSTI – RISKRECON ASSAULT – POPIS SLUŽBY (3/3)

Orientační harmonogram služby:

9:00 - 10:00: Úvodní schůzka s IT manažerem/majitelem.

10:00 - 12:00: Provedení počátečního průzkumu, analýza rizik, nastavení testovacího prostředí.

12:00 - 14:00: Testování síly antivirového softwaru a simulace ransomware útoku.
Ověření detekce odesílání dat a kontrola perimetrového firewallu

14:00 - 15:00: Analýza zabezpečení interních sítí a připojených zařízení.

15:00 - 16:00: Závěrečná schůzka s podrobným přehledem zjištěných informací a prvními doporučeními.

Do 3 pracovních dnů – Závěrečný report s nálezy a doporučením

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

ICYBEAR

EA-1. Motivace

EA-2. Strategie

EA-3. Operativa

EA-4. Informace

EA-5. Aplikace

EA-6. Data

EA-7. Sítě

EA-8. Aktiva

Využít můžete i naše další služby:

RED TEAMING – SIMULACE SOFISTIKOVANÝCH ÚTOKŮ:

- Simulace APT hrozeb – napodobujeme techniky používané státem sponzorovanými útočníky a sofistikovanými kyberzločinci. Obcházení bezpečnostních opatření – testujeme detekční schopnosti SOC, SIEM, EDR a XDR.
- Red teaming je proces, při kterém se tým odborníků (tzv. „red team“) pokouší napodobit chování potenciálního útočníka a identifikovat slabiny v systému, procesu nebo organizaci.
- Tento přístup se využívá v různých oblastech, jako je kybernetická bezpečnost, vojenská taktika, obchodní strategie nebo jiné oblasti rizikového managementu.
- V kybernetické bezpečnosti například red team vykonává simulované útoky na systém, aby odhalil zranitelnosti a slabiny, které by mohli zneužít skuteční hackeři. To zahrnuje testování obrany organizace, včetně sítě, aplikací, fyzické bezpečnosti a lidského faktoru (např. phishingové útoky).
- Red teaming se často kombinuje s „blue teamingem“, což je proces obrany proti těmto útokům. Když red team útočí, blue team se snaží odrazit útoky a zabezpečit systém.

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

ICYBEAR

EA-1. Motivace

EA-2. Strategie

EA-3. Operativa

EA-4. Informace

EA-5. Aplikace

EA-6. Data

EA-7. Sítě

EA-8. Aktiva

Využít můžete i naše další služby:

PHISHINGOVÉ KAMPANĚ:

- Cílené pihishingové kampaně – na základě našich reálně provedených útoků dosahujeme až 28% úspěšnosti v získání přihlašovacích údajů nebo spuštění škodlivého kódu.
- Analyzujeme lidský faktor, obcházíme bezpečnostní mechanismy a měříme reálnou míru ohrožení organizace.
- Phishing je typ kybernetického útoku pomocí technik sociálního inženýrství, při kterém se útočníci snaží získat citlivé informace (například hesla, čísla kreditních karet nebo osobní údaje) tím, že se vydávají za důvěryhodné instituce nebo jednotlivce.
- Nejčastěji se phishing provádí prostřednictvím e-mailů, které vypadají, jako by byly odeslány od známé společnosti (například banky, e-shopu nebo poskytovatele internetových služeb.

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

ICYBEAR

EA-1. Motivace

EA-2. Strategie

EA-3. Operativa

EA-4. Informace

EA-5. Aplikace

EA-6. Data

EA-7. Sítě

EA-8. Aktiva

Využít můžete i naše další služby:

PENETRAČNÍ TESTOVÁNÍ (AUTOMATIZACE + RUČNÍ PRÁCE):

- Externí a interní infrastruktura – testujeme reálné scénáře průniku. Active Directory & síťové útoky – Kerberoasting, NTLM relay, Golden Ticket, DCSync. Post-exploitation & laterální pohyb – analyzujeme, jak hluboko může útočník proniknout po kompromitaci.
- Asistované testy – spolupracujeme s vaším Security týmem a validujeme detekční mechanismy.
- Nejlepší automatizované skenery doplněné manuálním testováním – nezůstáváme jen u nástrojů, ale reálně ověřujeme zneužitelnost nalezených zranitelností.
- Penetrační testy (nebo také pen testy) jsou systematické testy, které simuluji útoky na informační systémy s cílem zjistit zranitelnosti a bezpečnostní slabiny.
- Tento proces zahrnuje simulaci reálného kybernetického útoku, aby se zjistilo, jak by útočník mohl proniknout do systému, získat citlivé informace nebo způsobit jinou škodu. Penetrační testy jsou součástí širšího rámce zajištění kybernetické bezpečnosti.

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

ICYBEAR

EA-1. Motivace

EA-2. Strategie

EA-3. Operativa

EA-4. Informace

EA-5. Aplikace

EA-6. Data

EA-7. Sítě

EA-8. Aktiva

Využít můžete i naše další služby:

3-HODINOVÝ WORKSHOP DIGITÁLNÍ BEZPEČNOSTI

Proč školení s námi?

- Aktuality: Seznámíme Vás s nejnovějšími hrozbami. Naučíme jak s hrozbami bojovat a na co si dát pozor. Jaké nástroje využívat. Bezpečnostní typy.
- Z praxe: Ukázka reálného útoku, jak hackeři postupují. Doporučení na bezpečnost doma s rodinou ale i ve firmě. Odhalení potenciálních rizik a škod.
- Analýza: Ukázka dostupnosti legálních informací. Hodnocení rizik a doporučení řešení napříč trhem.
- Akční cena: 8.000 KČ bez DPH. Max. 15 osob.

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

ICYBEAR

Naši experti se historicky v různých rolích a společnostech podíleli na implementaci špičkových řešení pro firmy a instituce.

Spolupracovali jsme s organizacemi, které vyžadují nejvyšší úroveň bezpečnosti a přesnosti.

- Více než 200 úspěšných projektů a 12 000+ zabezpečených zařízení.
- Více než 15 let zkušeností

Naše strategické partnerství s Gartner nám poskytuje nejnovější informace a analýzy, což nám umožňuje být vždy o několik kroků napřed před kyberútočníky.

ICYBEAR

REFERENCE NAŠICH EXPERTŮ

Pražská teplárenská

České dráhy

COLONNADE A FAIRFAX COMPANY

ČSÚ

Raiffeisen BANK

Úřad vlády České republiky

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

CERTIFIKACE NAŠICH EXPERTŮ

CEH Certified Ethical Hacker

CISA Certified Information Systems Auditor An ISACA Certification

eCPPT v2

TECHNOLOGIČTÍ PARTNEŘI

CHECK POINT

FORTINET

algotech

TREND MICRO

hp

Tomáš Havrda, Enterprise Architect, M: 602 275 207 E: tomas.havrda@ica-centrum.eu www.linkedin.com/in/tomashavrda

Nová éra kybernetické bezpečnosti

Děkuji za Váš čas a za Vaší pozornost. Prosím o Vaše otázky.

Ing. Tomáš Havrda

Enterprise Architect

M: 602 275 207

www.linkedin.com/in/tomashavrda

ICYBEAR
CYBER SECURITY