

Audit IT



Český institut
interních auditorů

Český institut interních auditorů, 3.11.2022

I. Proč provádět audit IT?

- Informační technologie – růst významu
- Prostřednictvím IS / IT se realizují veškeré účetní a většina obchodních činností
- Procházejí tudy veškeré informace v organizaci
- Roste objem prostředků vynakládaných na IT
- Za větší pohodlí se platí možnou větší napadnutelností systémů a technologií !
 - (Cloud, BYOD, Home Office...)

Kdo může provádět audit / kontrolu IT?

- Vnitřní (liniová) kontrola
- Interní / externí / outsourcovaný interní audit
- Penetrační test / Red teaming apod.

Možné základní typy auditů bezpečnosti v oblasti IS / IT

Je řada možných dělení auditů, např.:



Další typy auditů v oblasti IS / IT

Je řada možných dalších auditů, např.:

Audit řízení útvaru IT

Audit hospodaření útvaru IT

Audit licenční čistoty

Audit provozu útvaru IS / IT

Audit projektů IT a
rozvoje aplikací, změn. řízení

Další audity ...

Forenzní...

Odstraň.nedost...

II. Zákony a normy v oblasti ICT

Závazné zákonné normy

Nařízení GDPR

Zákon o kybernetické bezpečnosti 181/2014

Zákon o ISVS 365/2000

Prováděcí vyhlášky

Vyhláška 82/2018 (dříve 316/2014)

Vyhláška ČNB 163/2014

Normy (doporučení)

ČSN ISO/IEC 27001, 27002..

ITIL

ČSN EN ISO 9001

COBIT

Vnitřní normy organizace

Postup auditu

1. Obecně závazný předpis

2. Směrnice organizace

(Zahrnuje všechny obecně závazné předpisy? Není v rozporu s dobrou praxí, ale i se zdravým rozumem?)

3. Zjištěná skutečnost

(Odpovídá požadavkům směrnic? Jsou naplněny všechny požadavky směrnic? Nehrozí sankce za neplnění závazných předpisů? Není v rozporu s dobrou praxí, ale i se zdravým rozumem?)

Postup auditu - příklad

Vyhláška 82/2018 Sb. § 9

Audit bude hledat:

- (1) Povinná osoba v rámci řízení bezpečnosti lidských zdrojů
 - a) s ohledem na stav a potřeby systému řízení bezpečnosti informací stanoví **plán rozvoje bezpečnostního povědomí**, jehož cílem je zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí a který obsahuje formu, obsah a rozsah
 - 1. poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice a
 - 2. potřebných teoretických i praktických školení uživatelů, administrátorů a osob zastávajících bezpečnostní role,
 - b) **určí osoby odpovědné** za realizaci jednotlivých činností, které jsou v plánu uvedeny,
 - c) v souladu s plánem rozvoje bezpečnostního povědomí zajistí poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice formou **vstupních a pravidelných školení**,
 - d) pro osoby zastávající bezpečnostní role v souladu s plánem rozvoje bezpečnostního povědomí zajistí **pravidelná odborná školení**, přičemž vychází z aktuálních potřeb povinné osoby v oblasti kybernetické bezpečnosti,
 - e) v souladu s plánem rozvoje bezpečnostního povědomí zajistí **pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců** v souladu s jejich pracovní náplní,
 - f) zajistí kontrolu bezpečnostní politiky ze strany uživatelů

....

(2) Povinná osoba vede o školení podle odstavce 1 **přehledy**, které obsahují předmět školení a seznam osob, které školení absolvovaly.

Plán
rozvoje
bezpečno
stního
povědomí

Bezpečno
stní
politika

Docházka
na školení
A jeho
datum a
předmět

Kontrola
dodržován
í bezp.
politiky

Nová legislativa v oblasti ICT bezpečnosti - EU

Legislativa	Poznámka	Přijato	Účinnost cca
NIS2	(zřejmě se promítne do ZoKB) Více povinných práv.osob	Konec 2022	Polovina 2024
DORA		Konec 2022	2024
DSA / DMA		Červenec 2022	1.1.2024
ISO 27001, 27002:2022		Únor + Podzim 2022	V podstatě ihned
eIDAS 2.0	e – Wallet (e – Dokladovka v ČR zač. 2024)	Polovina 2023	Polovina 2025

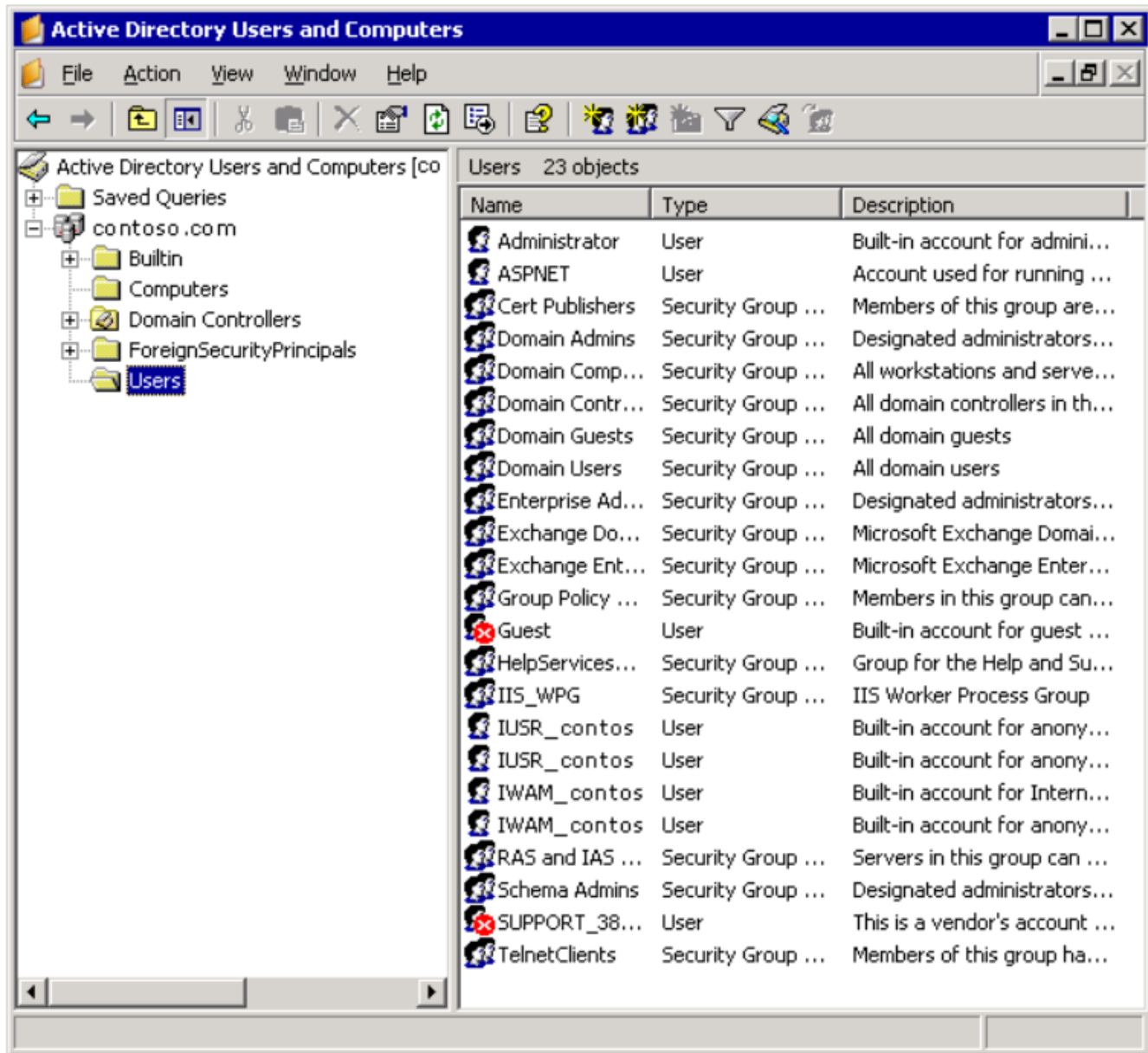
Nová legislativa v oblasti ICT bezpečnosti - ČR

Legislativa	Poznámka	Přijato	Účinnost cca
12/2020, O právu na digitální služby		Konec 2022	Zřízení DIA 1.1.2023, zrušení rodných čísel 31.12.2023
499/2004, O archivnictví		???	Pouze elektronická spisová služba 1.1.2026 Atestace ESS 1.7.2024, zřejmě změna na 1.1.2026
261/2021, „DEPO“	2021		
- 365/2000, o ISVS	2021	1.1.2023	Zavedení Katalogu cloud computingu
- 300/2008, o elektronických úkonech	2021		Datové schránky pro FOP 1.7.2023 (FO zřejmě NE)
- 250/2017, o elektronické identifikaci	2021	1.1.2022	Zavedení NIA

III. Příklad auditu - Prověrka přístupových práv

- ❖ V podstatě součást bezpečnosti systémů.
- ❖ Je však mnohem více propojena s administrativním zabezpečením, personálním útvarem atd.
- ❖ Její provedení je snazší, mechaničtější (i když může zároveň přinášet značnou pracnost)
- ❖ Zároveň má značný význam pro bezpečnost
- ❖ Přístupová práva se používají:
 - ❖ Na doméně Active Directory (nebo jiný LDAP)
 - ❖ Lokálně na serverech, stanicích, noteboocích
 - ❖ Při vzdáleném přístupu (VPN, VDI, RDP...)
 - ❖ V databázích
 - ❖ V jednotlivých aplikacích (nebo SSO)
 - ❖ Na aktivních prvcích
 - ❖ Atd. atd. atd.

Přístupová práva v doméně MS Windows



Windows domény jsou souborem objektů zabezpečení, které sdílejí centrální souborovou databázi. Tato centrální databáze je známá jako **Active Directory** a obsahuje uživatelské účty a informace o zabezpečení zdrojů v této oblasti. Každá osoba, která používá počítače v doméně, získá svůj vlastní účet nebo uživatelské jméno. Tomuto účtu je pak umožněn přístup ke zdrojům v rámci domény.

Rychlé získání přehledu o uživateli – pro audit výhodné

- Např. použitím příkazu NET z příkazové řádky.
- Postup:
- Spustit přes CMD nebo COMMAND Příkaz.
Řádek
- Zadat NET USERS /DOMAIN
- Popřípadě lze přímo zachytit do souboru, např. NET USERS /DOMAIN >c:\prava.txt
- Takový soubor se dá načíst např. do MS EXCELu

Microsoft Excel - prava_srovnani.xls

Soubor Úpravy Zobrazit Vložit Formát Nástroje Data Okno Nápověda

Nápověda – zadejte dotaz

Arial 10 B I U

G21 Biedermann Denis

	G	H	I	J	K	L	M	N	O
93		hruskova	hruskova						
94	Hrušková Marie	hruskovam	hruskovam						
95	Hýblová Monika	hyblova	hyblova						
96	Chludilová Danuše	chludilova	chludilova						
97	Chmelenská Miluše								
98	Chyšková Anna	chyskova	chyskova						
99		llS servis							

```

1 C:\WINDOWS\system32\cmd.exe
1 testWKS1          testWKS2          tollner
1 tovek            trebinova        trenda
1 trnka            trnkova          trucova
1 trzil            TsInternetUser  tuckova
1 turdik          ucebna0          ucebna1
1 ucebna10        ucebna11        ucebna12
1 ucebna2         ucebna3          ucebna4
1 ucebna5         ucebna6          ucebna7
1 ucebna8         ucebna9          unzeitig
1 urbankova      vaclavek        vaclavik
1 vana            vandasova       vavrova
1 vcislakova     velin            vesely
1 vetrovec       vitova          vlcek
1 vmezl          vnukovai        voglova
1 vokrova        volfova         vomlelova
1 vondracek      vratnice        vyplelova
1 vyvoj2provoz   zahradnik       zcap
1 zubrik         zvolensky       ZZ_AddComp
1 ZZ_imoblogon   zz_logon        ZZ_xplogon
1 ZZ_xplogon_ts  zz_xpterminal
14 Příkaz byl úspěšně dokončen.
P
  
```

123

Start Kontr_Juran_... 7 Internet E... dochazka.xls Microsoft Exce... Servant Salam... C:\WINDOWS... 18:52

Formální postup přidělení práv

ZADOST O: PRIDELENÍ – ZMENU – ZRUSENÍ PRISTUPOVYCH PRAV
(nehodící se škrtněte)

Jméno _____
Odbor _____
Právo požadováno od _____
Popis přístupu k aplikaci / adresáři

Přístup: čtení zápis
Odůvodnění

+ Změnu navrhl (uživatel)

Jméno	Funkce	Datum	Podpis

Změnu potvrdil (ředitel odboru)

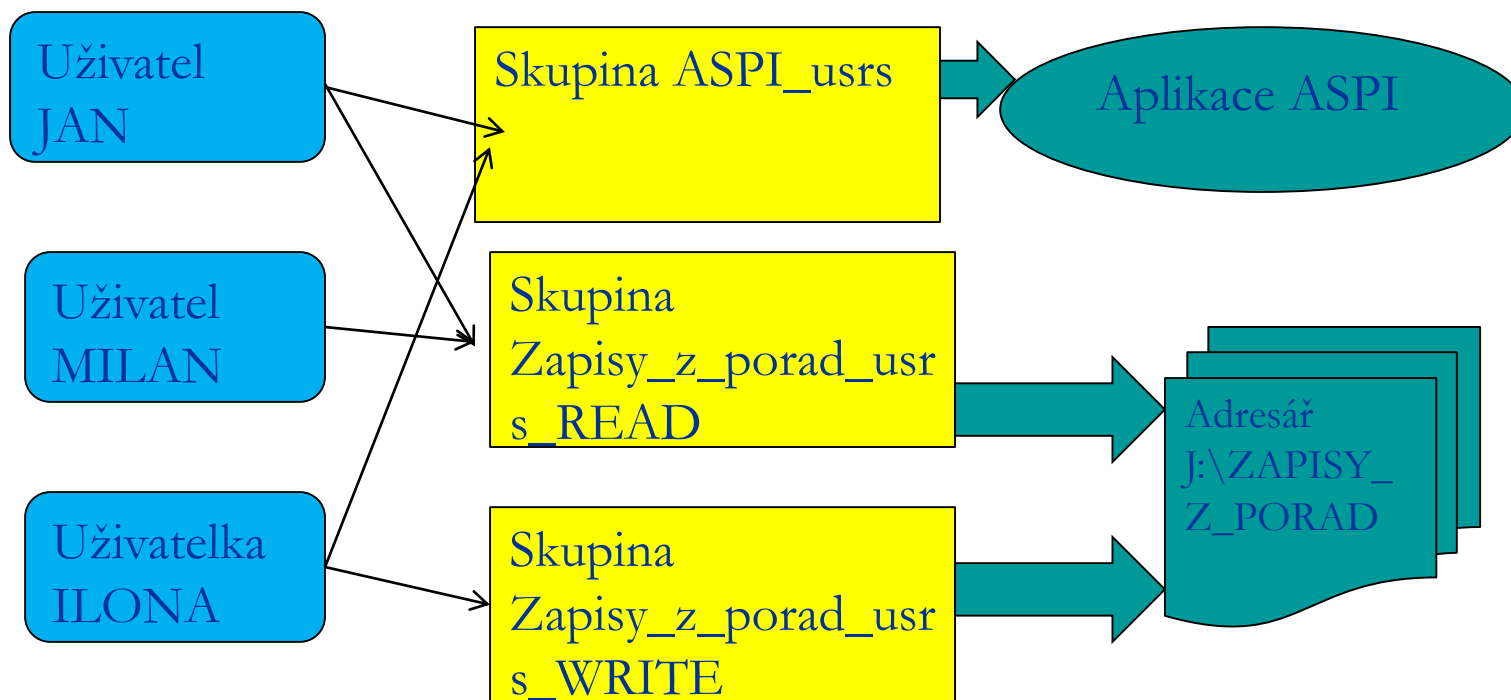
Jméno	Funkce	Datum	Podpis

Změnu schválil (odbor bezpečnosti IT)

Jméno	Funkce	Datum	Podpis

Uživatelé x skupiny

- Správný postup: práva k objektům se přiřazují skupinám, ne přímo jednotlivým uživatelům!



Seznam skupin a jejich předpokládaného naplnění

Skupina	Popis skupiny	Přístupy skupině přidělené	Předpokládaní uživatelé	Skutečnost / Rozdíl
US-1K	Mapování Q:\	Aplikace Skladové hospodářství.	Účtárna	2 pracovníci účtárny a V. Roth na základě sdělení odboru 5000 z 28.4.2011. OK.
US-ALIT_R	Komise ALIT	Adresář J:\ALIT čtení	Členové ALIT, audit, dle požadavku předsedy ALIT z 8.3.2010 též dealing	<u>Navíc mají přístup Škába (už není členem komise) a Javorský.</u>
US-ALIT_RW	Komise ALIT	Adresář J:\ALIT zápis	Předseda a tajemník komise	Odpovídá
US-Audit	Audit - sledování plnění napravných opatření	Adresář J:\AUDIT a aplikace IS_AUDIT	Členové PŘ, NGR, ŘO	Odpovídá. <u>ŘO 1100 Ing. Adam práva nemá přidělena (nemůže reagovat na zjištění auditu).</u>

IV. Audit ochrany proti malware a dalším útokům

- Základní obranou může být např.:
 - Antivir
 - Firewall
 - Proxy server, Mailová GW
 - IDS / IPS
 - Sandbox
 - EDR /XDR
 - SIEM / SOAR
- Dále též režimová opatření – CSIRT, Threat Intelligence, Red Teaming, Penetrační testy apod.

Ransomware



Ooops, your files have been encrypted! English

What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send \$300 worth of bitcoin to this address:

bitcoin ACCEPTED HERE

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

- Soubory jsou zašifrovány.
- K jejich odšifrování je požadováno zaplatit „výkupné“.
- Zašifruje se všude, kam má konkrétní uživatel přístup (i na síti!)

Ochrana stanic

- Slouží k ochraně koncových stanic před škodlivým kódem a průnikem útočníka. **Od běžných antivirových produktů se liší logováním důležitých aktivit na koncové stanici a širokými možnostmi při řešení incidentu.**
- Řešení EDR umožňuje sbírat informace o aktivitách na koncové stanici, například informace o:
 - **rodičovských procesech,**
 - **vykonaných příkazech přes příkazový řádek nebo powershell,**
 - **stažených souborech a jejich reputaci,**
 - **změnách v registrech,**
 - **DNS requestech a obecně síťové komunikaci,**
 - **změnách v souborovém systému.**
- Analytik díky EDR systému získá možnost vzdáleného připojení na koncovou stanici a může tak **vynutit ukončení škodlivého procesu, smazat soubory či si je stáhnout pro detailní analýzu nebo kompletně zablokovat síťovou komunikaci** infikované stanice.

Ochrana stanic – Antivir, EDR a DLP

Konzole avast! Distributed Network Manager, May2007

Soubor Zobrazení PgDlače Účpověda

Nastavení Nová Změnit

Složky Workstations

Jméno	verze VPS	Verze jádra	Operač...	Poslední komunikace	Poslední virus
PC_PWC	080307-0, 07.03.2008	4.7.700.0	Window...	březen, 7 (pátek)	<žádný virus nenalezen>
ODO	080410-1, 10.04.2008	4.7.801.0	Window...	duben, 11 (pátek)	<žádný virus nenalezen>
PC_SLO2	080430-1, 30.04.2008	4.7.820.0	Window...	duben, 30 (středa)	<žádný virus nenalezen>
PC_LIST	080505-0, 05.05.2008	4.7.801.0	Window...	květen, 6 (úterý)	<žádný virus nenalezen>
SVA	080506-0, 06.05.2008	4.7.801.0	Window...	květen, 7 (středa)	<žádný virus nenalezen>
PC_XXX	080508-0, 08.05.2008	4.7.820.0	Window...	květen, 9 (pátek)	<žádný virus nenalezen>
PC_DVO	080511-0, 11.05.2008	4.7.801.0	Window...	květen, 12 (pondělí)	<žádný virus nenalezen>
PC_MASE	080515-0, 15.05.2008	4.7.801.0	Window...	čtvrtek, 16:53:49	<žádný virus nenalezen>
MDN	080515-0, 15.05.2008	4.7.801.0	Window...	čtvrtek, 16:33:04	<žádný virus nenalezen>
PC_1AN	080515-0, 15.05.2008	4.7.801.0	Window...	čtvrtek, 15:10:33	<žádný virus nenalezen>

avast! Administráční konzole

Úlohy

- Klientské úlohy
- Residentní skenovací úlohy (c)
- Skenovací úlohy na vyžádání
- Aktualizační úlohy
- Instalační úlohy
- Pomocné úlohy
- Serverové úlohy
- Úlohy Hledání počítačů
- Správa databáze
- Reportovací úlohy

Seance

- Residentní skenery
- Lokální skenery
- Lokální síťové štyby
- Klientské úlohy
- Serverové úlohy

Katalog počítačů

- Servers
- Workstations
- Dynamické skupiny počítačů
- Management servery
- Uživatelé
- Varování
- Plánovač
- Instalační balíčky
- Události

Struktura složek

avast! Administráční konzole

Úlohy

Seance

Katalog počítačů

Servers

Workstations

Dynamické skupiny počítačů

Management servery

Uživatelé

Varování

Plánovač

Události

Složka obsahuje 130 položek, 0 z nich je vybrány...

Start

2 M, 4 M, Ser..., Přík..., Aid..., Mic..., HP..., DM..., Ko..., CS, 14:47

SIGNALS PROCESS GRAPH

Process File Socket Registry DNS Lookup Lateral Movement

/bin/bash /tmp/sample.sh

/tmp/sample.sh

sh -c rm ... /dev/null 2>&1

/tmp/sample.elf

getent passwd

rm /usr/bin/fs.cop

/tmp/sample.elf

grep -v ... /tmp/sample.elf

Data Loss Prevention Reports > Incidents (last 7 days)

Workflows Remediate Escalate

Report: Incidents (last 7 days) Date Range: Last 7 days Manage Report

ID	Incident Time	Source	Polices	Channel	Destination	Severity	Action	Maximum Matches	Transaction Size	Status
215794	21 May 2016, 10:53:51 AM	Sun Tau	Project FP Policy...	Network email	domain@for...	Medium	Attachment(s) dropped	3	2.57 MB	New
217168	25 May 2016, 07:02:23 PM	hannibal barba	US Credit Cards...	HTTPS	data.kaltest.com	High	Permitted	43	47.8 KB	New
217089	25 May 2016, 06:26:12 PM	hannibal barba	Web DLP Policy, U...	HTTPS	data.kaltest.com	High	Permitted	1	31 B	New
216920	25 May 2016, 05:50:26 PM	hannibal barba	Web DLP Policy, US P...	HTTPS	data.kaltest.com	High	Permitted	2	88 B	New
216079	25 May 2016, 05:24:23 PM	for...	Email DLP Policy	network email	800.com	Medium	Quarantined	2	55.7 KB	New
215777	25 May 2016, 04:40:46 PM	Sun Tau	Web DLP Policy, S...	HTTPS	data.kaltest.com	High	Permitted	1	21 B	New
214958	25 May 2016, 03:21:11 PM	Sun Tau	Web DLP Policy	HTTPS	data.kaltest.com	High	Permitted	2	88 B	New
214830	25 May 2016, 02:46:03 PM	hannibal barba	Web DLP Policy	HTTPS	data.kaltest.com	High	Permitted	13	950 B	New
213969	25 May 2016, 02:16:47 PM	hannibal barba	US Credit Cards...	HTTPS	data.kaltest.com	High	Permitted	43	47.8 KB	New
214734	25 May 2016, 01:57:37 PM	hannibal barba	US Credit Cards...	HTTPS	data.kaltest.com	High	Permitted	39	12.99 MB	New

Incident: 215794 Severity: Medium Action: Attachment(s) d... Tune Policy

Deploy: Violation triggers

Rule: Attachment type

- Microsoft Visio File - All Versions (File Type) 2
- DC Water: WebSense between Diagram.vsd, objObject1.bin 1
- Microsoft Office File - Non-Web-Protected (File Type) 1
- WebSense Web Security Gateway Deployment Plan for DC Water - Draft L 1
- Microsoft Office File - All Versions (File Type) 2
- WebSense Web Security Gateway Deployment Plan for DC Water - Draft L 1
- Microsoft Office File (File Type) 1
- WebSense Web Security Gateway Deployment Plan for DC Water - Draft L 1

Rule: Project FP Policy

- Project's Fingerprinting (Predefined Fingerprinting - File & Directories) 1
- \\tsk\share\DL\Fingerprinting\services\DC Water\ntkrb5e Web Secur...

Incident Details

Severity: Medium

Status: New

Action: Attachment(s) dropped

Channel: Network email

Analyzed by: Policy Engine espia

Detected by: TRITON AP-EPAL on espia

Event time: 31 May 2016, 03:52:51 AM

Incident time: 31 May 2016, 10:53:51 AM

Assigned to: Unassigned

Incident tag: N/A

Max matches: 3

Source

Full name: Sun Tau *

Email address: suntau@nabz

Login name: suntau *

Destination

Email address:

* This was not one of the event's original properties. It was determined through user name resolution.

Ukázka ACL – access control listu

- `access-list 100 permit tcp any gt 1023 host 192.168.122.100`
- `access-list 100 permit ip any 192.168.102.0 0.0.0.255`
- `access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.102.0 0.0.0.255`
- `access-list 100 permit tcp any eq 443 host 192.168.122.100`
- `access-list 100 permit ip any host 192.168.122.100 log`
- **`access-list 100 deny ip any any log`**

untangle DASHBOARD APPS CONFIG REPORTS HELP ACCOUNT

Default Rack > Firewall

Status Rules Reports

Note
Routing and Port Forwarding functionality can be found elsewhere in Config->Networking.

Rules

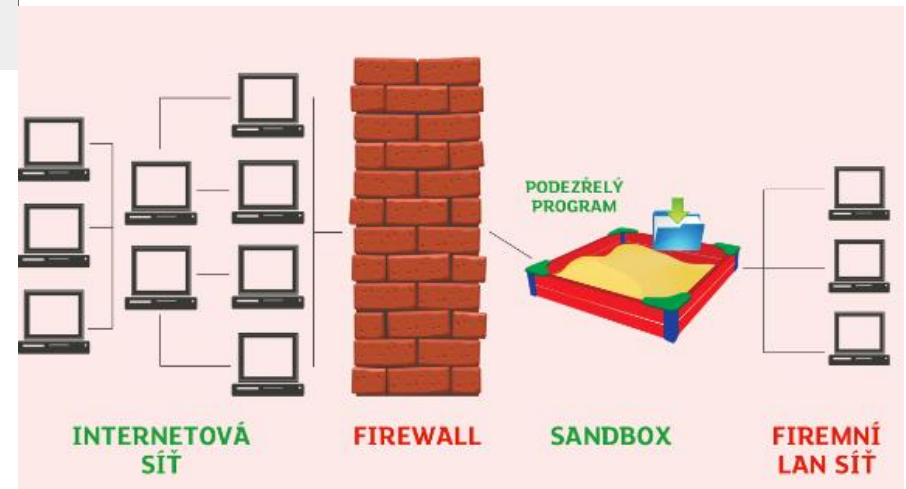
+ Add Import Export

Rule Id	Enable	Description	Block	Flag	Reorder	Edit	Delete
100001	<input type="checkbox"/>	Block and flag all traffic destined to port 21	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	↕	📄	✕
100002	<input type="checkbox"/>	Block and flag all TCP traffic from 1.2.3.0 netmask 255.255.255.0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	↕	📄	✕
100003	<input type="checkbox"/>	Accept and flag all traffic to the range 1.2.3.1 - 1.2.3.10 to ports 1000-5000	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	↕	📄	✕
100004	<input type="checkbox"/>	block QUIC	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	↕	📄	✕
100005	<input type="checkbox"/>	block 172.16.2.10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	↕	📄	✕

Remove Help OK Cancel Apply

Proxy server, e-mailová GW a sandbox

Whitelist/Blacklist	Quarantine Settings	Spam Settings	Password
Spam Filter Enable/Disable Save Changes ?			
Enable Spam Filtering: <input checked="" type="radio"/> Yes <input type="radio"/> No		If No , all messages will be delivered without being scanned for spam. Recommended: Yes	
Spam Scoring Save Changes ?			
Use System Defaults: <input checked="" type="radio"/> Yes <input type="radio"/> No		If No , you must specify the scoring levels that you would like to use below. Recommended: Yes	
A score is calculated for each incoming email to determine the likelihood of spam. 0 = not spam 9 = definitely spam			
Tag:	3.5	Score at which subject line is modified. Recommended: 3.5	
Quarantine:	4	Set to 10 to disable quarantine. Recommended: 10	
Block:	7	Set to 10 to disable blocking. Recommended: 7	



IDS / IPS a SIEM

Vulnerability Info

Vulnerability description

Many popular MIME-compliant email clients are vulnerable to a denial of service attack caused by a buffer overflow in the handling of certain headers. By sending a specially-crafted mail message, an attacker can overflow a buffer and crash another user's client. It may be possible to use this vulnerability to execute arbitrary commands on the victim's computer.

How to remove this vulnerability

Upgrade to the latest version of Sendmail (8.9.1a or later), as listed in CERT Advisory CA-1998-10. See References.

For Microsoft Outlook: Apply the appropriate patch for your system, as listed in Microsoft Security Bulletin MS98-008. See References.

For other distributions: Contact your vendor for upgrade or patch information.

References

Microsoft Security Bulletin MS98-008
Update Available For 1.0nn file

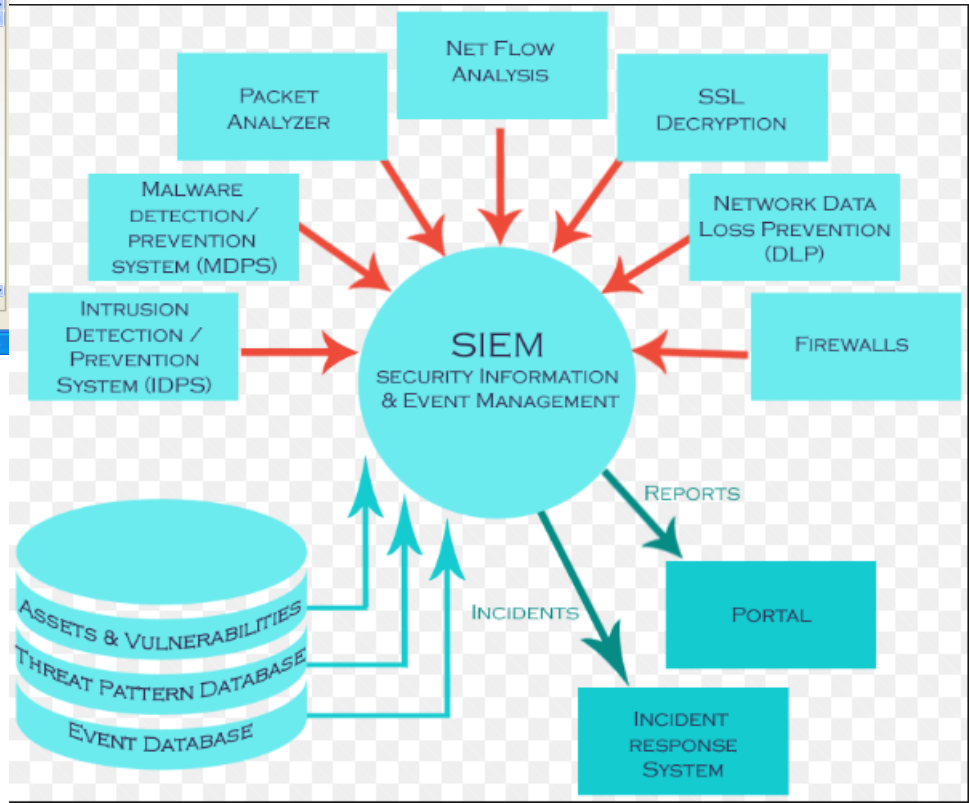
Analysis

9-05-13 00:00:00 CEST Start: [] End: [] Target IP: []

Analysis - Details (Agent)

Tag Name	Event Count	Status	Severity	Source IP
18:05:26 CEST Email_Exchange_Mime_Decoding	1	Detected event (SecurityFusion not...	High	172.22.202.10
16:05:48 CEST Email_Mime_Filename_Overflow	1	Detected event (SecurityFusion not...	High	172.22.200.21
10:41:14 CEST HTML_UTF8_Overflow	1	Detected event (SecurityFusion not...	High	193.86.238.33
01:39:05 CEST Email_Executable_Extension	1	Detected event (SecurityFusion not...	Medium	172.22.202.10
03:37:07 CEST Email_Executable_Extension	1	Detected event (SecurityFusion not...	Medium	172.22.202.10
03:37:07 CEST Email_Executable_Extension	1	Detected event (SecurityFusion not...	Medium	172.22.202.10
03:37:07 CEST Email_Executable_Extension	1	Detected event (SecurityFusion not...	Medium	172.22.202.10
03:37:07 CEST Email_Executable_Extension	1	Detected event (SecurityFusion not...	Medium	172.22.202.10
03:37:07 CEST Email_Executable_Extension	1	Detected event (SecurityFusion not...	Medium	172.22.202.10
03:37:07 CEST Email_Executable_Extension	1	Detected event (SecurityFusion not...	Medium	172.22.202.10
03:37:07 CEST Email_Executable_Extension	1	Detected event (SecurityFusion not...	Medium	172.22.202.10
03:37:07 CEST Email_Executable_Extension	1	Detected event (SecurityFusion not...	Medium	172.22.202.10
03:37:07 CEST Email_Executable_Extension	1	Detected event (SecurityFusion not...	Medium	172.22.202.10
03:37:07 CEST Email_Executable_Extension	1	Detected event (SecurityFusion not...	Medium	172.22.202.10
03:37:07 CEST Email_Executable_Extension	1	Detected event (SecurityFusion not...	Medium	172.22.202.10
03:37:07 CEST Email_Executable_Extension	1	Detected event (SecurityFusion not...	Medium	172.22.202.10
03:37:07 CEST Email_Executable_Extension	1	Detected event (SecurityFusion not...	Medium	172.22.202.10
03:37:07 CEST Email_Executable_Extension	1	Detected event (SecurityFusion not...	Medium	172.22.202.10
03:37:07 CEST Email_Executable_Extension	1	Detected event (SecurityFusion not...	Medium	172.22.202.10
08:00:55 CEST Email_Executable_Extension	1	Detected event (SecurityFusion not...	Medium	172.22.200.21
08:38:37 CEST Email_Executable_Extension	1	Detected event (SecurityFusion not...	Medium	172.22.202.10
08:38:46 CEST Email_Executable_Extension	1	Detected event (SecurityFusion not...	Medium	172.22.202.10
09:19:34 CEST Email_Executable_Extension	1	Detected event (SecurityFusion not...	Medium	172.22.200.21
10:48:56 CEST Email_Executable_Extension	1	Detected event (SecurityFusion not...	Medium	172.22.200.21
12:00:40 CEST Email_Executable_Extension	1	Detected event (SecurityFusion not...	Medium	172.22.202.10
12:06:53 CEST HTTP_Head	1	Detected event (SecurityFusion not...	Medium	172.22.200.21
12:15:32 CEST Email_Executable_Extension	1	Detected event (SecurityFusion not...	Medium	172.22.202.10

403 rows with 1 selected. spadmin



Postup auditu

- Pro interní audit poměrně komplikované, jde o sofistikovaná zařízení.
- Možný postup:
 - nechat si předložit logy (za několik dní) a politiky
 - nebo vyjít ze známého bezpečnostního incidentu, a zajímat se o to, proč nebyl včas zachycen
 - při auditu funkce síťových zařízení začít vždy od přístupu na Internet a mail běžných uživatelů
 - je vhodné se zaměřit na zastaralé údaje (již neexistující uživatelé, stanice, URL adresy, IP adresy nebo zastaralé virové definice, chybějící běžné situace v politikách, pravidla pro již neexistující logy v SIEMu apod.)
 - nebo se opřít o Bezpečnostní politiku popř. vyhlášku 82/2018 Sb. (např. §18 - firewall, § 21 – antivir, § 22 – SIEM, § 24 – IDS apod.)
 - Viz např. §22 odst.2d vyhlášky (SIEM má zajistit zaznamenávání:)
 1. přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů,
 2. činností provedených administrátory,
 3. úspěšné i neúspěšné manipulace s účty, oprávněními a právy,
 4. neprovedení činností v důsledku nedostatku přístupových práv a oprávnění,
 5. činností uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému,
 6. zahájení a ukončení činností technických aktiv,
 7. kritických i chybových hlášení technických aktiv a
 8. přístupů k záznamům o událostech, pokusy o manipulaci se záznamy o událostech a změny nastavení nástrojů pro zaznamenávání událostí a
- **Porovnat, zda požadavky splňuje úplně, zda zařízení vykazuje situace určitého ohrožení, zda se to ihned reportuje nebo alertuje apod.**

Dotazy?



Děkuji Vám za pozornost !