Audit IT

Český institut interních auditorů, 3.11.2022

Ing. Jan Bukovský, jan.bukovsky@ceb.cz

I. Proč provádět audit IT?

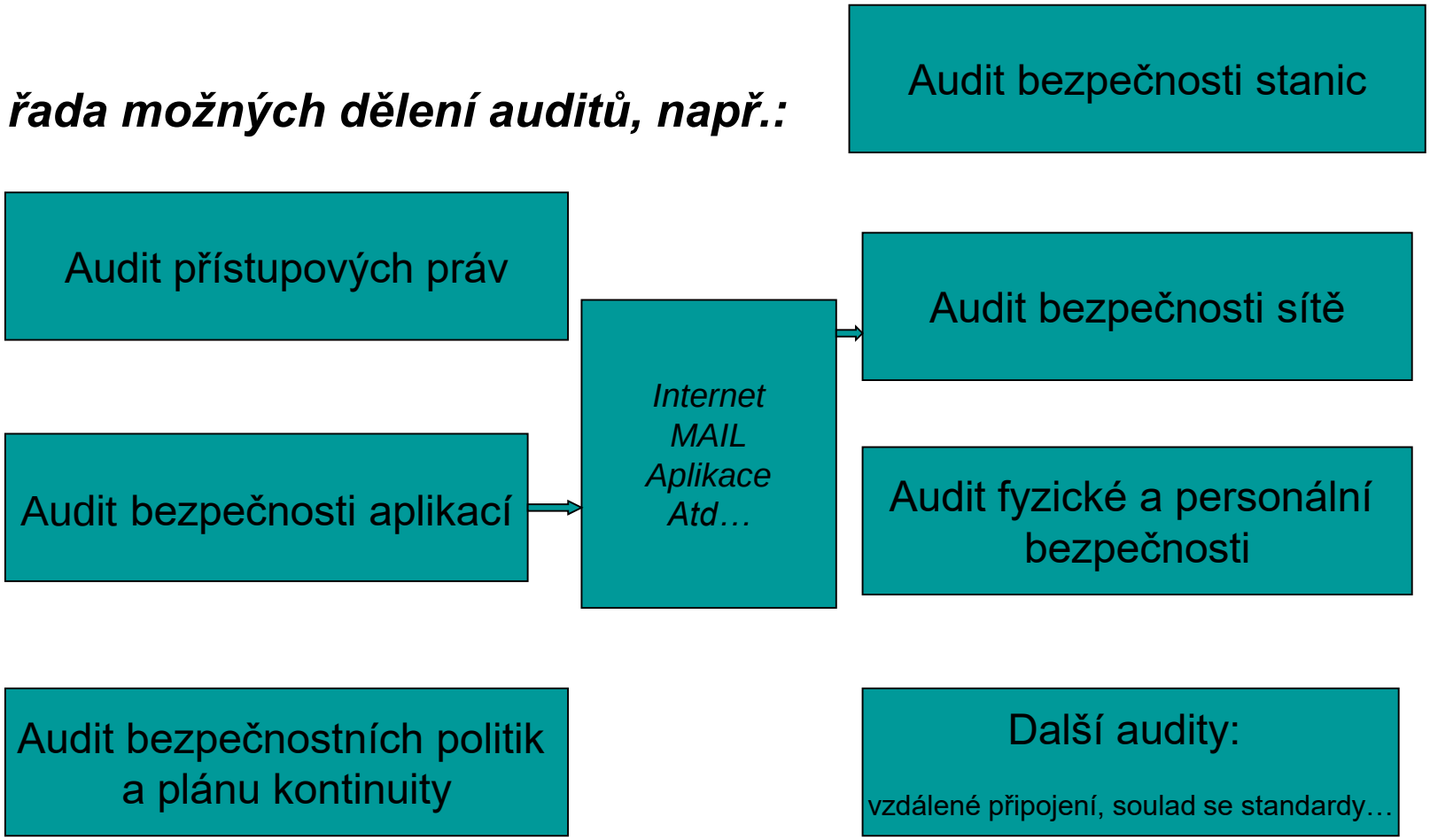
- Informační technologie – růst významu
- Prostřednictvím IS / IT se realizují veškeré účetní a většina obchodních činností
- Procházejí tudy veškeré informace v organizaci
- Roste objem prostředků vynakládaných na IT
- Za větší pohodlí se platí možnou větší napadnutelností systémů a technologií !
 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

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

- *(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.

Audit bude hledat:

- **Plán rozvoje bezpečnostního povědomí**
- **Docházka na školení A jeho datum a předmět**
- **Bezpečnostní politika**
- **Kontrola dodržování 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

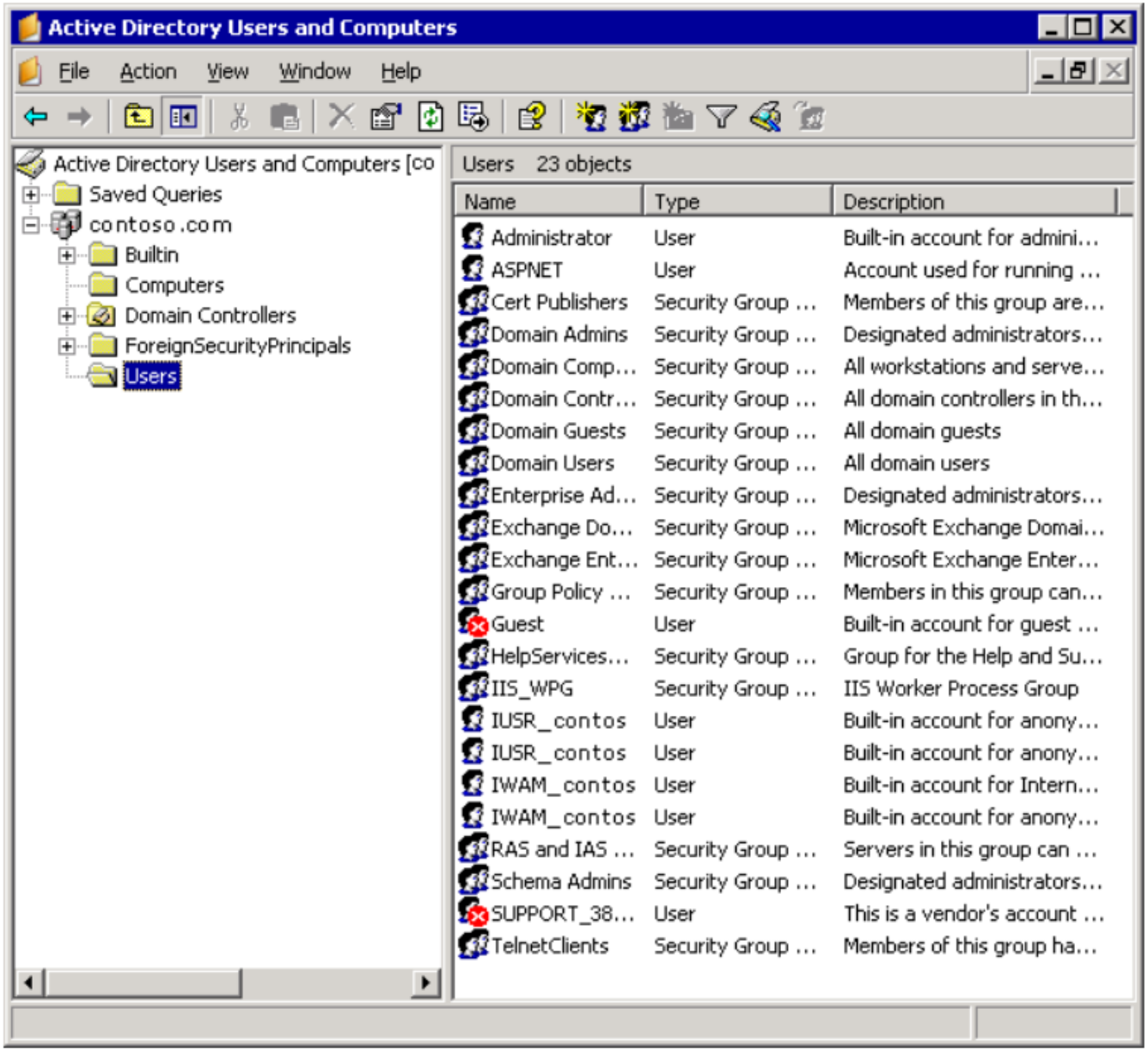
Nová legislativa v oblasti ICT bezpečnosti - ČR

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

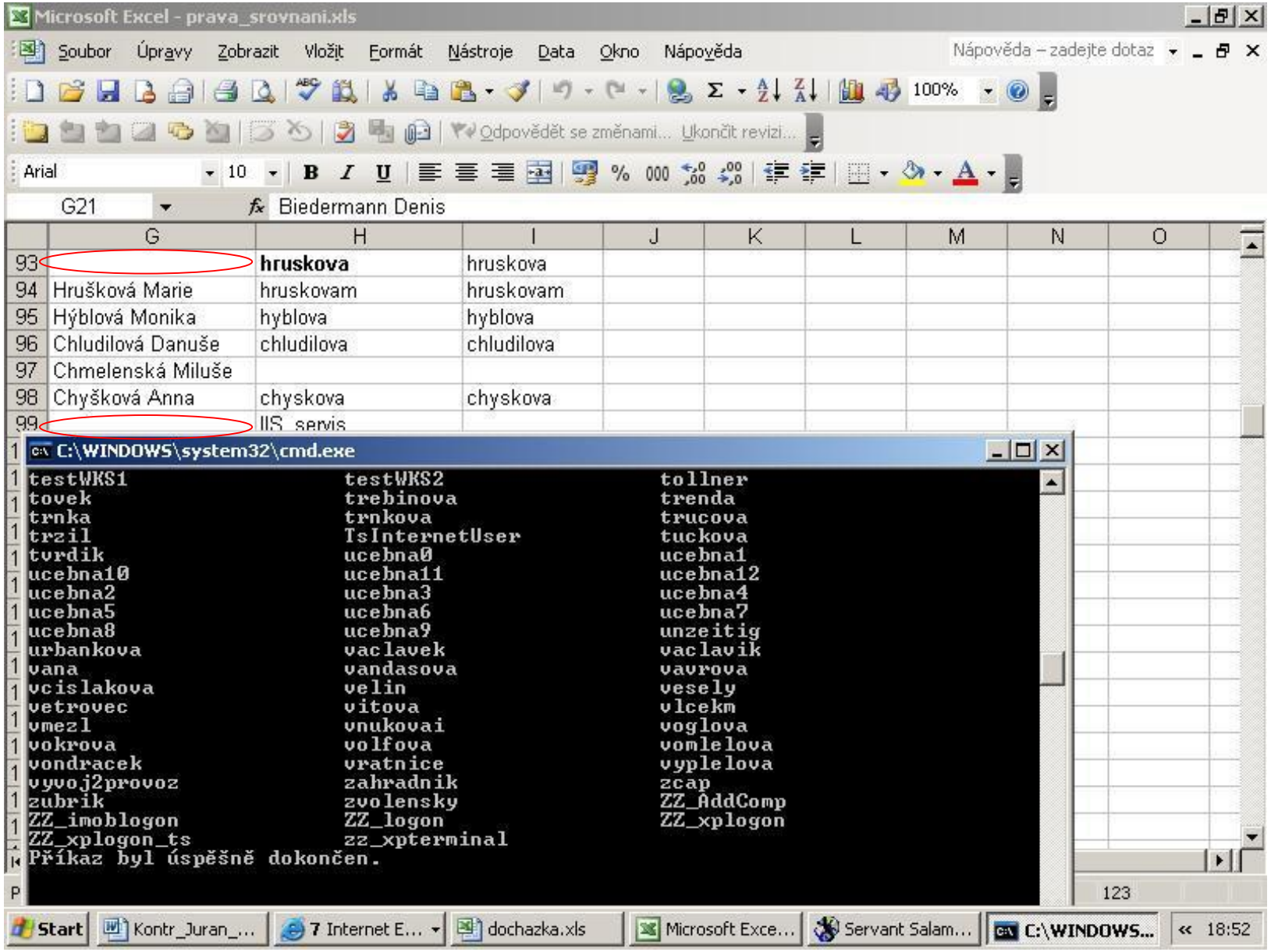


Windows domény jsou souborem objektů zabezpečení, které sdílejí centrální souborovou databázi. Tato centrální databáze je známá jako **Active Directory** a obsahuje uživatelské účty a informace o zabezpečení zdrojů v této oblasti. Každá osoba, která používá počítače v doméně, získá svůj vlastní účet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

Ing. Jan Bukovský,
jan.bukovsky@ceb.cz

Rychlé získání přehledu o uživatelích – 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
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 IIS_servis
C:\WINDOWS\system32\cmd.exe
testWKS1 testWKS2 tollner
tovek trebinova trenda
trnka trnkova trucova
trzil TsInternetUser tuckova
tvrdik ucebna0 ucebna1
ucebna10 ucebna11 ucebna12
ucebna2 ucebna3 ucebna4
ucebna5 ucebna6 ucebna7
ucebna8 ucebna9 unzeitig
urbankova vaclavek vaclavik
vana vandasova vavrova
vcislakova velin vesely
vetrovec vitova vlcekm
vmezl vnukovai voglova
vokrova volfova vomlelova
vondracek vratnice vyplelova
vyvoj2provoz zahradnik zcap
zubrik zvolensky ZZ_AddComp
ZZ_imoblogon ZZ_logon ZZ_xplogon
ZZ_xplogon_ts zz_xpterminal
Příkaz byl úspěšně dokončen.
123
Start
Kontr_Juran_...
7 Internet E...
dochazka.xls
Microsoft Exce...
Servant Salam...
C:\WINDOWS...
18:52

Formální postup přidělení práv

ZADOST O: PRIDELENI – ZMENU – ZRUSENI 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

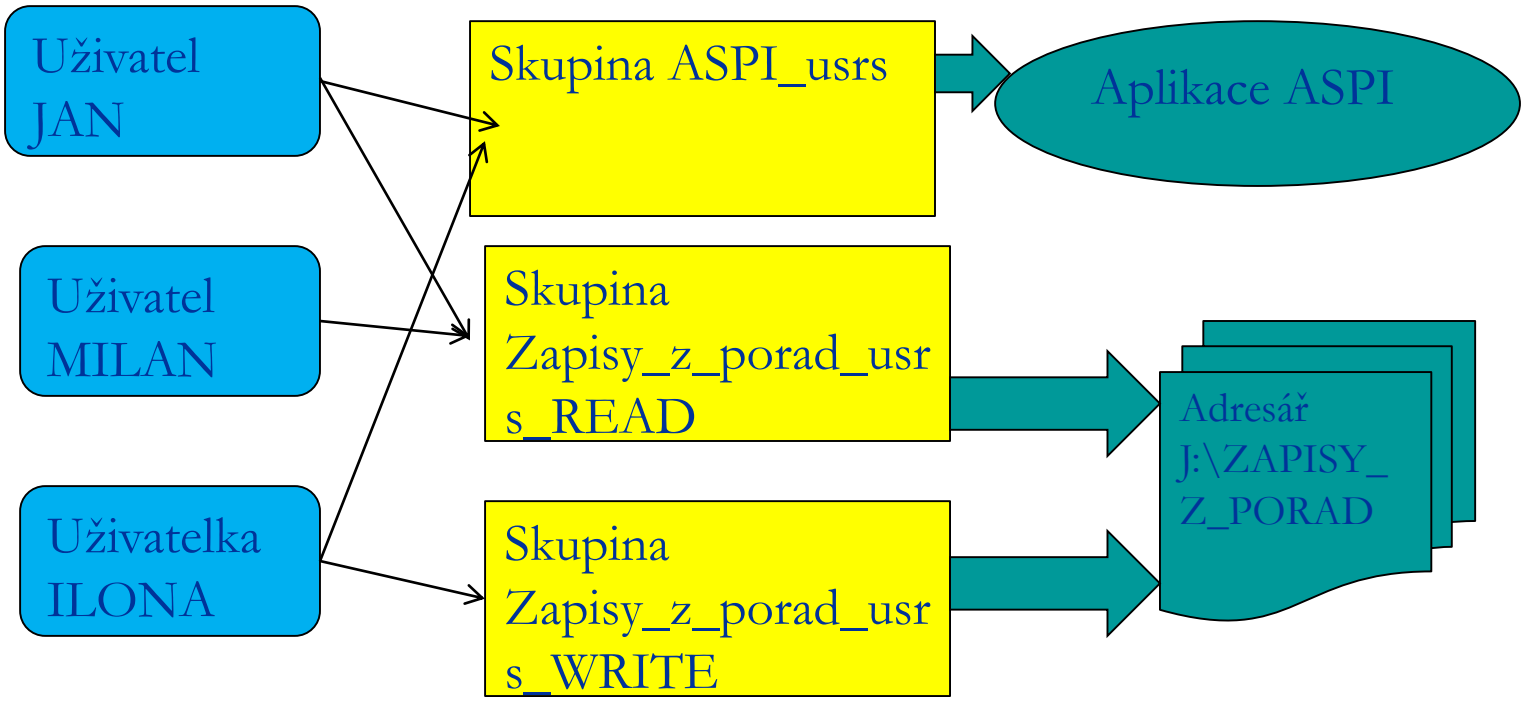
Změnu schválil (odbor bezpečnosti IT)

Jméno	Funkce	Datum	Podpis

Ing. Jan Bukovský, jan.bukovsky@ceb.cz

Uživatelé x skupiny

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

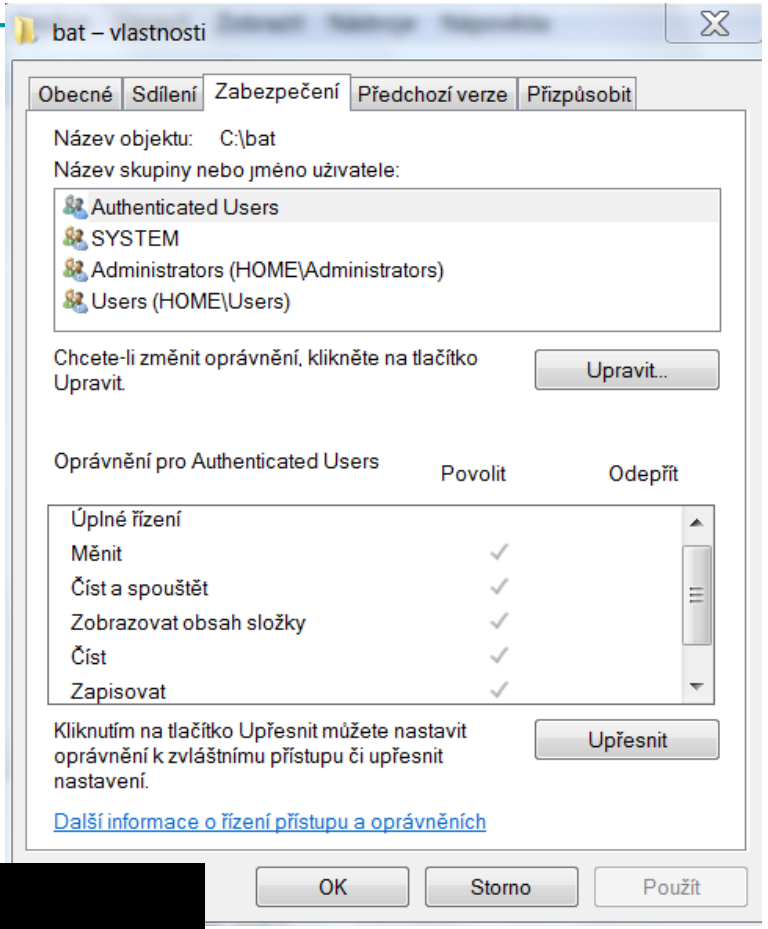


Seznam skupin a jejich předpokládaného naplnění

Skupina	Popis skupiny	Přístupy přidělené skupině	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	**Navíc mají přístup Škába (už není členem komise) a Javorský.**
US-ALIT_RW	Komise ALIT	Adresář J:\ALIT zápis	Předseda a tajemník komise	**Odpovídá**
US–Audit	Audit - sledovani plneni napravnych opatreni	Adresář J:\AUDIT a aplikace IS_AUDIT	Členové PŘ, NGŘ, ŘO	**Odpovídá.** **ŘO 1100 Ing. Adam práva nemá přidělena (nemůže reagovat na zjištění auditu).**

Přístupová práva k souborům a adresářům

CACLS C:\BAT*.*
F full, R read, W write
ID zděděno, CI práva budou dědit podřízené adresáře, OI práva budou dědit podřízené soubory




```
C:\bat\auto>cacls *.*
C:\bat\auto\AUTOMAT1.BAT BUILTIN\Administrators:(ID)F
                         NT AUTHORITY\SYSTEM:(ID)F
                         BUILTIN\Users:(ID)R
                         NT AUTHORITY\Authenticated Users:(ID)C

C:\bat\auto\AUTOMAT2.BAT BUILTIN\Administrators:(ID)F
                         NT AUTHORITY\SYSTEM:(ID)F
                         BUILTIN\Users:(ID)R
                         NT AUTHORITY\Authenticated Users:(ID)C

C:\bat\auto\AUTOMAT3.BAT BUILTIN\Administrators:(ID)F
                         NT AUTHORITY\SYSTEM:(ID)F
                         BUILTIN\Users:(ID)R
                         NT AUTHORITY\Authenticated Users:(ID)C

C:\bat\auto\AUTOMAT4.BAT BUILTIN\Administrators:(ID)F
                         NT AUTHORITY\SYSTEM:(ID)F
                         BUILTIN\Users:(ID)R
                         NT AUTHORITY\Authenticated Users:(ID)C
```

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.

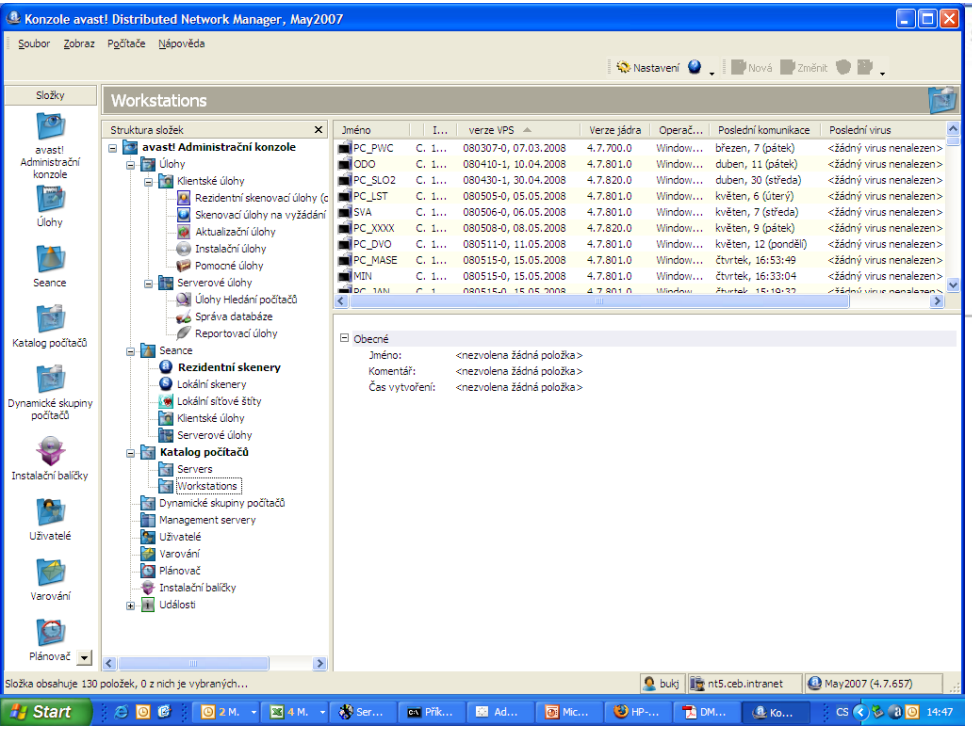
Ransomware

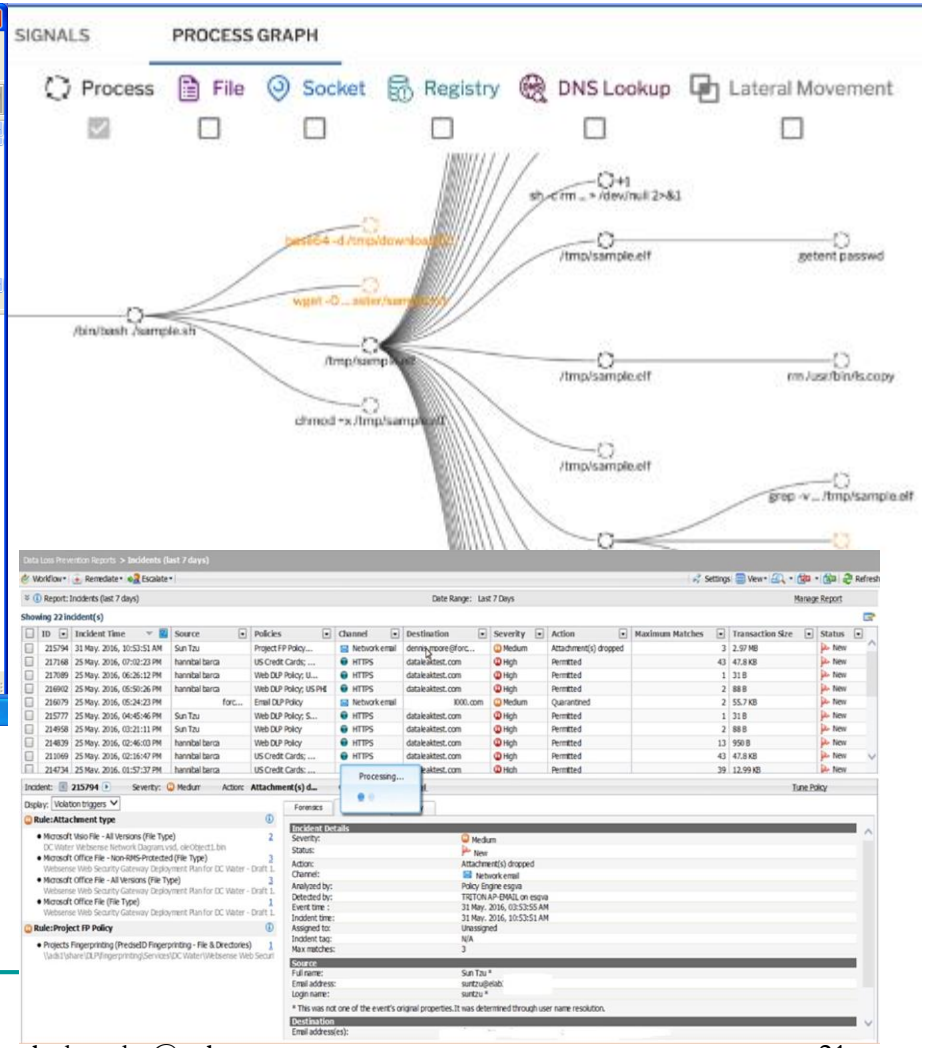
- Soubory jsou zašifrovány.
- K jejich odšifrování je požadováno zaplatit „výkupné“.
- Zašifruje se všude, kam má konkrétní uživatel přístup (i na síti!)

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.

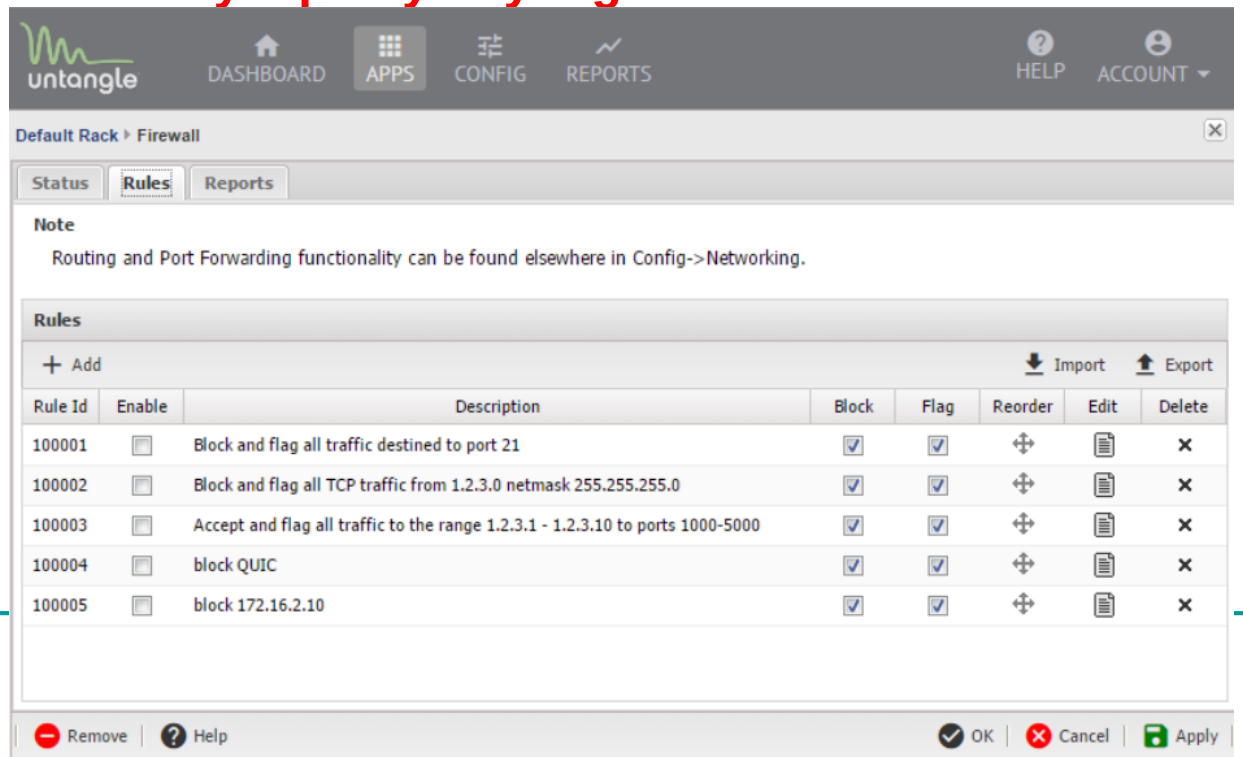
Ochrana stanic – Antivir, EDR a DLP





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**



Proxy server, e-mailová GW a sandbox

Whitelist/Blacklist | Quarantine Settings | Spam Settings | Password

Spam Filter Enable/Disable Save Changes ?

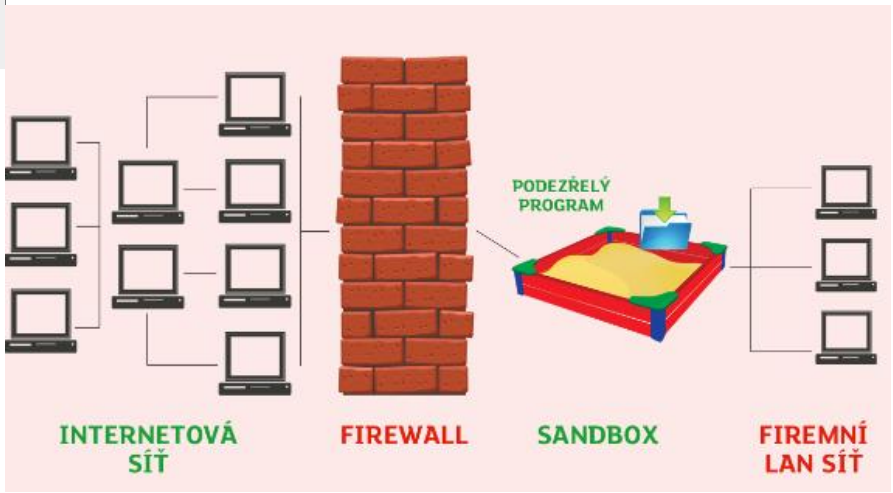
Enable Spam Filtering: (•) Yes ( ) No — If **No**, all messages will be delivered without being scanned for spam. **Recommended**: Yes

Spam Scoring Save Changes ?

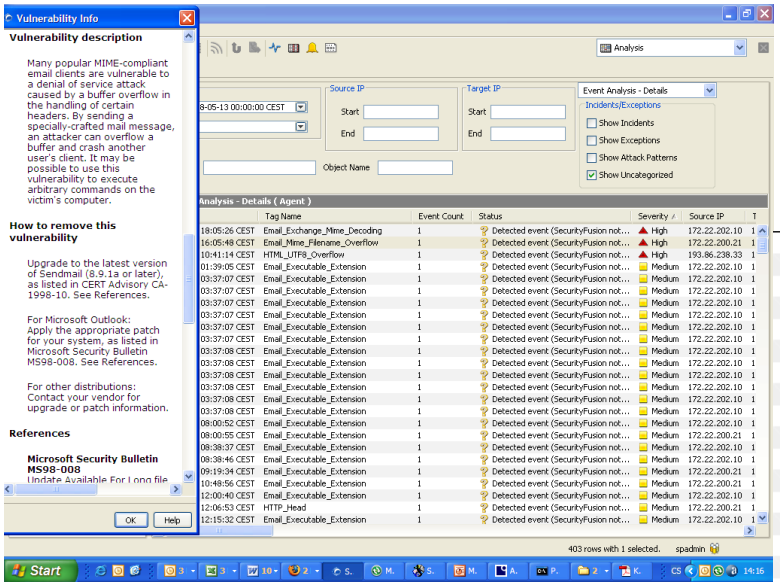
Use System Defaults: (•) Yes ( ) No — If **No**, you must specify the scoring levels that you would like to use below. **Recommended**: Yes

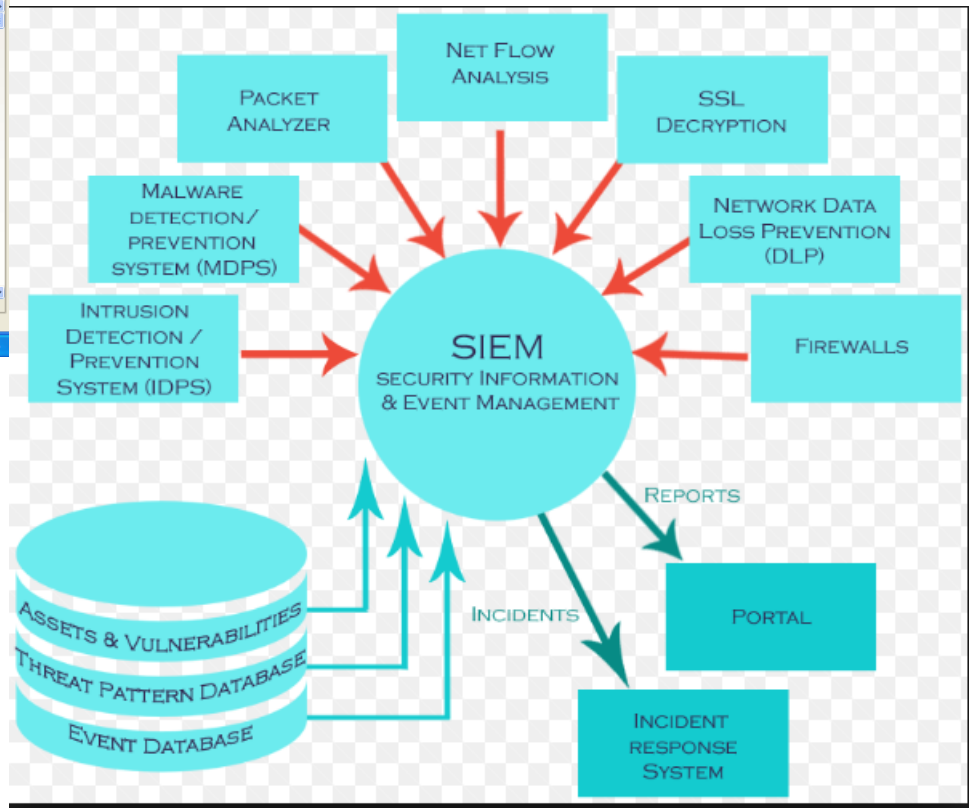
A score is calculated for each incoming email to determine the likelihood of spam.
0 = not spam 9 = definitely spam

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





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 !