

SECURITY 2012



20. ročník konference o bezpečnosti v ICT

Praktické a efektivní řízení zranitelnosti IS

Martin HANZAL

SODATSW spol. s r.o.





Obsah příspěvku

- Teoretický úvod do problematiky řízení zranitelnosti
- Proč bychom zranitelnost měli řídit
- Kde se takové řízení nachází v organizaci
- Praktické příklady řízení zranitelnosti



Představení autora

- Martin HANZAL je současným výkonným ředitelem společnosti SODATSW spol. s r.o., která od roku 1997 pomáhá technickými prostředky zvyšovat ochranu informací v rámci informačních systémů nejrůznějších organizací
- Zaměření především na ochranou důvěrnosti a integrity zpracovávaných dat a monitoringu podporujícího nepopiratelnost operací
- Člen NATO Industry Advisory Group v rámci vedení NATO v Bruselu, sekce Cyber Defence, vede skupinu Research&Technology



Zranitelnost

- Není to nic nového, řeší se odpradáвна
- Kdo zvládá minimalizovat zranitelnosti, ten dosahuje lepších výsledků
- Zranitelnost není možné odstranit jednou pro vždy, protože většinou závisí na vývoji dalších okolností
- Je nutné se jí zabývat v rámci kontinuálního procesu v organizaci



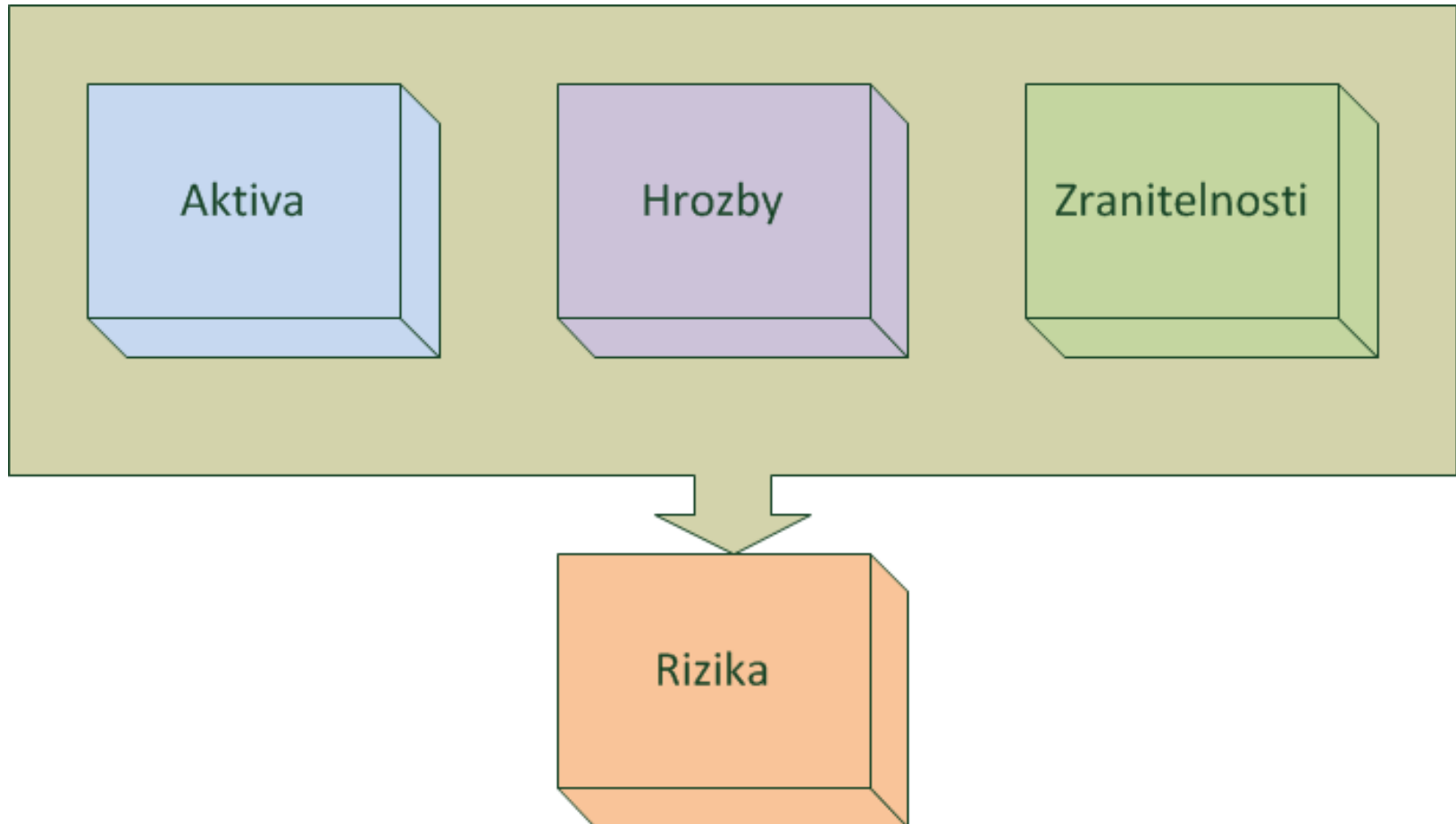
Achillova pata

- I to se dá považovat za řízení rizika, při kterém zůstalo jen jedno slabé místo





Risk management



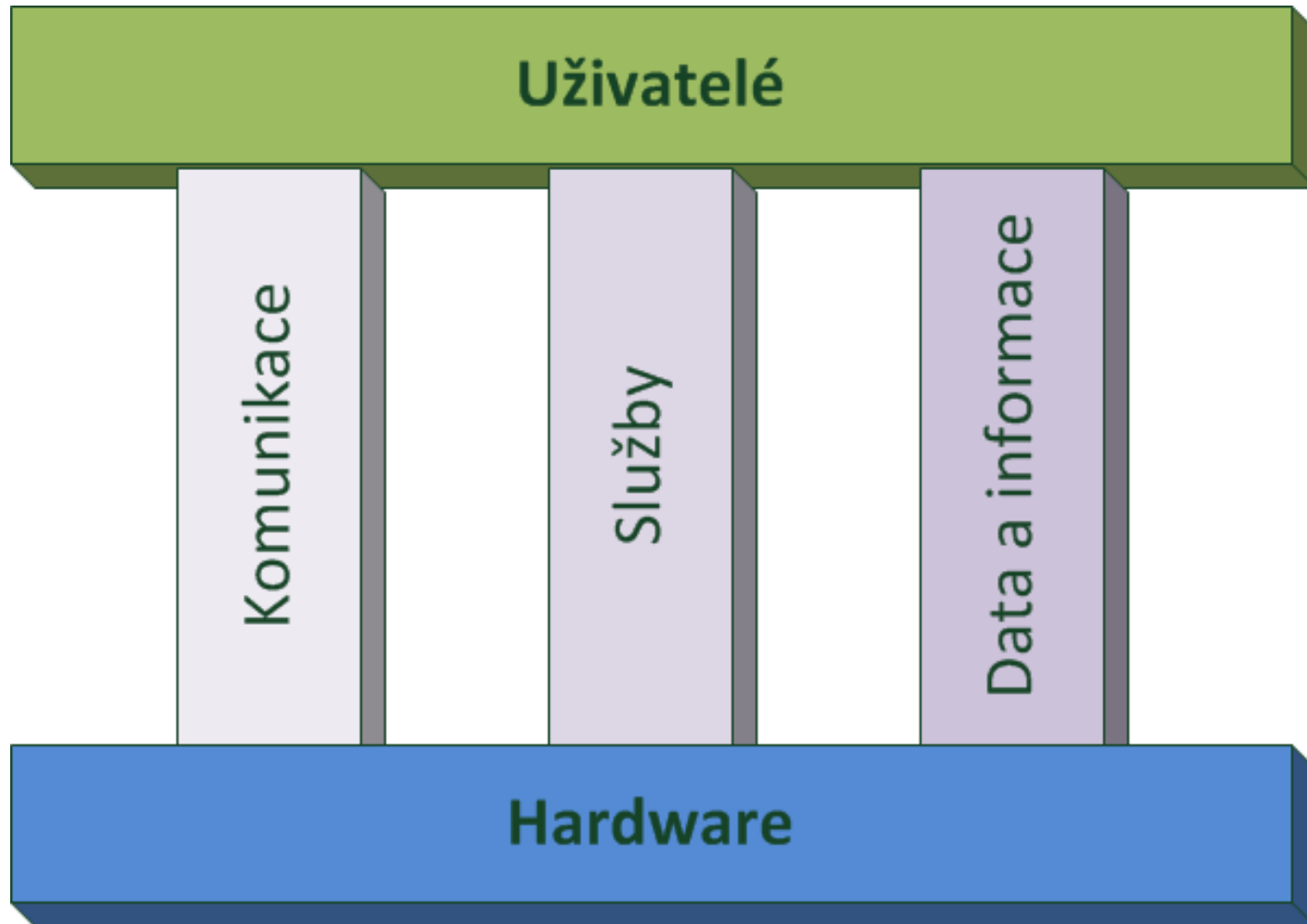


Zranitelnost IS

- V rámci risk managementu je nutné posuzovat pro každé aktivum IS
- Známe-li příslušnou zranitelnost aktiva, pak můžeme navrhnout úměrná protiopatření
- V současných IS je nejdůležitější hodnocení zranitelnosti hlavně z pohledu dat, informací a služeb, provozovaných v rámci IS
- Řízení zranitelnosti je kontinuální proces, který je možné velmi dobře řídit v rámci ISMS



Architektura IS





Role řízení zranitelnosti

- Při řízení rizik se aktiva a hrozby mění jen minimálně, ale zranitelnosti vznikají nové, původní se vyvíjí a zanikají
- Je nutné přesně definovat role zodpovědností za hodnocení zranitelnosti
- Zodpovědnost za řízení je na straně IT manažera
- Každodenní práce je na straně IT administrátorů

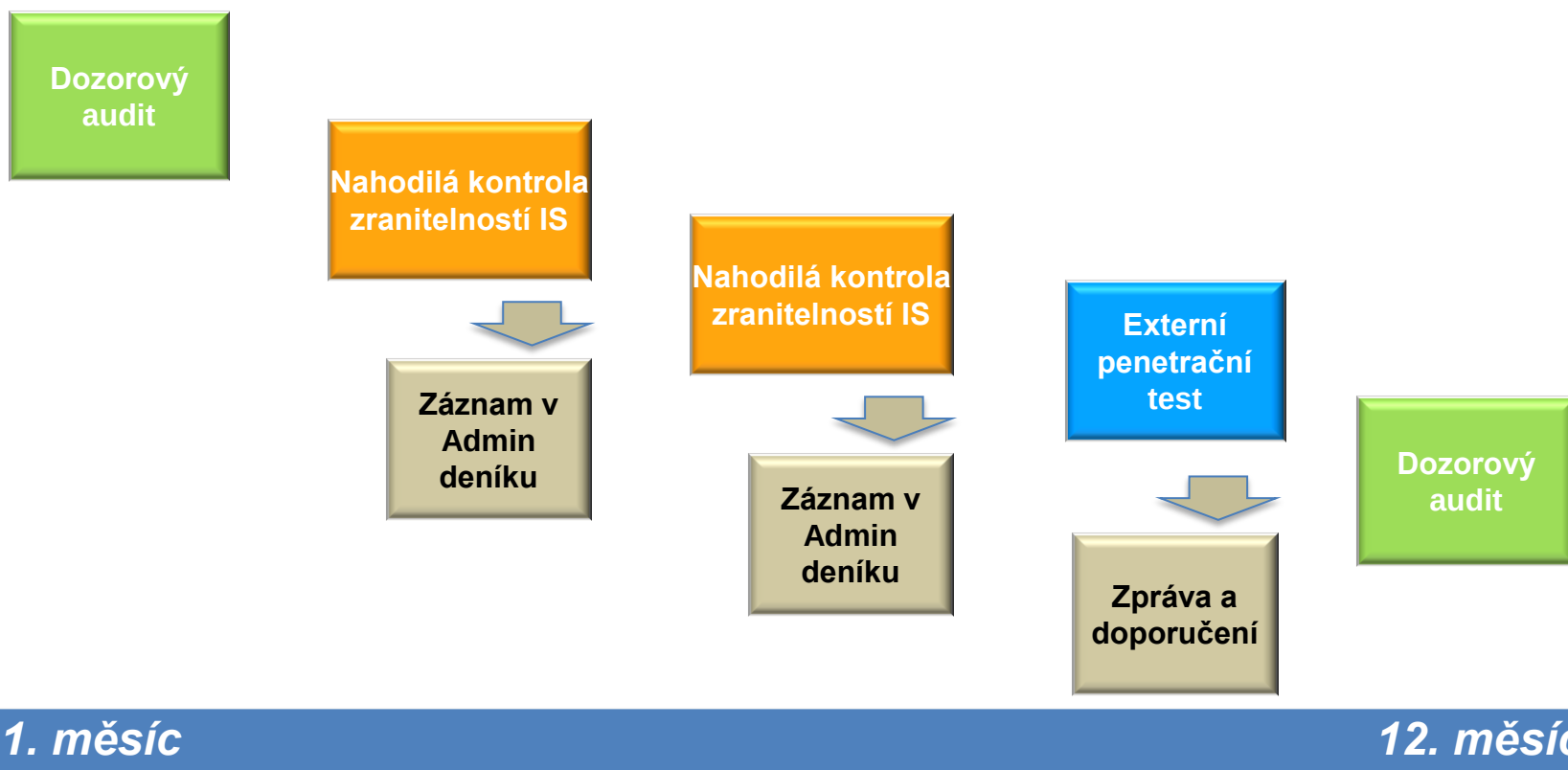


Scénáře řízení zranitelnosti

- Zavedení do každodenního provozu není ze dne na den a je zapotřebí od zavádění řízení zranitelnosti neustupovat
- Organizace bez ISMS řízení dělají ad-hoc (a jsou stále tací, kteří nedělají)
- Organizace s ISMS, kteří mají jen papírovou bezpečnost, tak mnohdy něco udělají jen kvůli auditu
- Organizace s žijícím ISMS mají řízení zranitelnosti zakotveno v celkovém řízení organizace

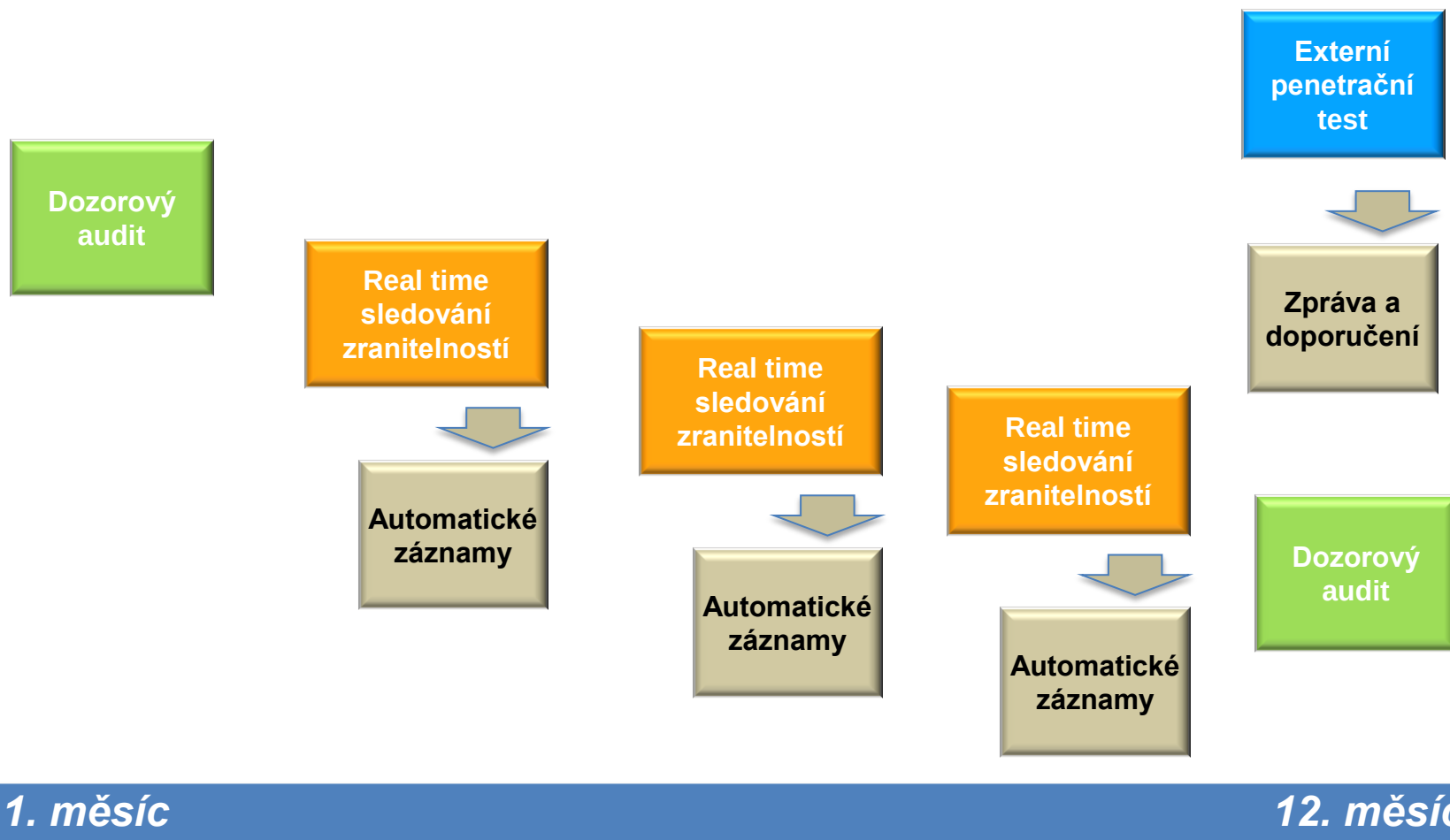


Pasivní ISMS





Žijící ISMS





Automatické řízení zranitelnosti

- Při výběru technologií posuzovat, jestli vybíraná technologie je schopna sledovat a reportovat svoje stavy, především
 - Aktuálnost komponent
 - Nastavení
 - Činnost za určité období
 - Anomálie
- Zdokumentovat proces, co se je nutné z pohledu zranitelností sledovat



Pokročilé řízení

- Jedná se o systémy Security Information and Event Management (SIEM)
- Je zapotřebí zvážit nutnost a přínos investic do pokročilého řízení zranitelnosti
- Přehnané požadavky bývají kontraproduktivní, protože ve výsledku nikdo neví, jak má na všechny poplachy reagovat, takže nereaguje



Příklad řízení aktuálních verzí

AreaGuard Neo
Soubor Průvodci Nástroje Info

Počítače Skupiny Uživatelé

Vybrané období 5.1.2012 - 5.2.2012

Stav stanic
14
14

Aktivita stanice
17
11

Jméno skupiny: sodatsw Počet PC: 74
Cesta ke skupině: sodatsw Počet uživatelů: 174

Typ	Datum a čas	Uživatel	Počítač	Vyhodnocení	Popis
✗			NB-DEVELOP03	Stav systému	Systém není nainstalován správně Aktuálních balíčků: 0 Špatných balíčků: 2 Poslední kontrola stanice před: 82 dní a 10:37:9
✗			NB-MH-VIS	Stav systému	Systém není nainstalován správně Aktuálních balíčků: 0 Špatných balíčků: 2 Poslední kontrola stanice před: 509 dní a 4:29:10
✗			NB-PD02	Stav systému	Probíhá odinstalace Aktuálních balíčků: 0 Špatných balíčků: 2 Poslední kontrola stanice před: 303 dní a 7:11:31
✗			NB-PM05	Stav systému	Systém není nainstalován správně Aktuálních balíčků: 0 Špatných balíčků: 3 Stanice je aktivní
✓			NT01	Stav systému	Systém je nainstalován Aktuálních balíčků: 3 Špatných balíčků: 0 Stanice je aktivní
✓			NT02	Stav systému	Systém je nainstalován Aktuálních balíčků: 3 Špatných balíčků: 0 Stanice je aktivní
✓			NT03	Stav systému	Systém je nainstalován Aktuálních balíčků: 3 Špatných balíčků: 0 Stanice je aktivní
✓			NT04	Stav systému	Systém je nainstalován Aktuálních balíčků: 4 Špatných balíčků: 0 Stanice je aktivní
✓			NT05	Stav systému	Systém je nainstalován Aktuálních balíčků: 3 Špatných balíčků: 0 Stanice je aktivní
✓			NT06	Stav systému	Systém je nainstalován Aktuálních balíčků: 3 Špatných balíčků: 0 Stanice je aktivní

Hledat
Hledat v: Vše

Strana: 1 / 2



Příklad řízení aktuálních verzí

AreaGuard Neo

Soubor Průvodci Nástroje Info

Počítače Skupiny Uživatelé

soDATSW

Správa klientů Výměnná zařízení Lokální adresáře Sdílená data Klíče Diagnostika

Vybrané období 5.1.2012 - 5.2.2012

Stav stanice
14
14

Aktivita stanice
17
11

Jméno skupiny: soDATSW
Počet PC: 74
Cesta ke skupině: soDATSW
Počet uživatelů: 174

Typ	Datum a čas	Uživatel	Počítač	Vyhodnocení	Popis
✗			NB-DEVELOP03	Stav systému	Systém není nainstalován správně Aktuálních balíčků: 0 Špatných balíčků: 2 Poslední kontrola stanice před: 82 dní a 10:37:9
✗			NB-MH-VIS	Stav systému	Systém není nainstalován správně Aktuálních balíčků: 0 Špatných balíčků: 2 Poslední kontrola stanice před: 509 dní a 4:29:10
✗			NB-PD02	Stav systému	Probíhá odinstalace Aktuálních balíčků: 0 Špatných balíčků: 2 Poslední kontrola stanice před: 303 dní a 7:11:31
✗			NB-PM05	Stav systému	Systém není nainstalován správně Aktuálních balíčků: 0 Špatných balíčků: 3 Stanice je aktivní

Statistiky
Poslední známý uživatel: SODATSW/martino
Poslední známá aktivita: 4.2.2012 17:26
Poslední kontrola stavu stanice: 2.2.2012 9:45
Přítí kontrola stavu stanice: 2.2.2012 13:45

Seznam balíčků:

Jméno balíčku	Stav	Verze	Požadovaná verze	Instalace požadované verze	Výsledek instalace požadované verze
AreaGuard Neo - Installer	Upgrade	1.3.1348.0	1.3.1349.500	-	-
AreaGuard Neo - Client	Upgrade	1.3.1348.0	1.3.1349.500	-	-
AreaGuard Neo - Logon	Upgrade	1.3.1348.0	1.3.1349.500	-	-

Přejít na kartu počítače

✓			NT01	Stav systému	Systém je nainstalován Aktuálních balíčků: 3 Špatných balíčků: 0 Stanice je aktivní
✓			NT02	Stav systému	Systém je nainstalován Aktuálních balíčků: 3 Špatných balíčků: 0 Stanice je aktivní

Hledat v: Vše

Strana: 1 / 2

Zajištění důvěrnosti dat

AreaGuard Neo

Soubor Průvodci Nástroje Info

Počítače

Skupiny Uživatelé

sodatsw

Vybrané období 5.1.2012 - 5.2.2012

Data v lokacích	Používaná data mimo lokace	Nepoužívaná data mimo lokace
131,73 GB 412,8 MB	151,31 GB	125,97 GB

Jméno skupiny: sodatsw Počet PC: 74
Cesta ke skupině: sodatsw Počet uživatelů: 174

Typ	Datum a čas	Uživatel	Počítač	Akce	Popis
⚠	3.2.2012 17:45:44		PC-NAHRADNI04	Nezašifrovaná data v lokacích	Počet lokací: 2
⚠	3.2.2012 14:20:46		W8-1	Nezašifrovaná data v lokacích	Počet lokací: 3
⚠	3.2.2012 8:50:47		NT01	Nezašifrovaná data v lokacích	Počet lokací: 1
⚠	2.2.2012 16:20:33		NT14	Nezašifrovaná data v lokacích	Počet lokací: 2
⚠	2.2.2012 13:52:03		NT04	Nezašifrovaná data v lokacích	Počet lokací: 3

Obsah souborů:

Kategorie	Velikost dat	Nejčastější lokace	Nejčastější typ	Využíváno dat
Aplikace/Systém	640,17 MB	D:\	Binárky/Systém	17,33 %
Internet	132,22 MB	C:\Users\denism\	Internet	3,58 %
Kancelářské balíky	995,36 MB	C:\Users\denism\	Pošta	26,94 %
Multimédia	1,65 GB	D:\	Grafické formáty	45,94 %
Ostatní	229,76 MB	C:\Users\denism\	Ostatní	6,22 %

Seznam lokací:

Cesta	Šifrováno klíčem	Stav zašifrování	Velikost dat
C:\Users\miroslav\	miroslav_Personal_000	94,66 %	21,43 MB
C:\Users\denism\	denism_Personal_001	99,57 %	1,63 GB
D:\	denism_Personal_001	100 %	1,95 GB

Typ	Datum a čas	Uživatel	Počítač	Akce	Popis
⚠	27.1.2012 8:12:30		NT05	Nezašifrovaná data v lokacích	Počet lokací: 3
⚠	24.1.2012 11:01:35		NT08	Nezašifrovaná data v lokacích	Počet lokací: 4
✓	3.2.2012 7:10:40		PC03	Data v lokacích v pořádku	Počet lokací: 1
✓	2.2.2012 10:11:47		NT02	Data v lokacích v pořádku	Počet lokací: 2
✓	2.2.2012 9:11:36		NT03	Data v lokacích v pořádku	Počet lokací: 2
✓	1.2.2012 8:08:29		NT09	Data v lokacích v pořádku	Počet lokací: 2
✓	31.1.2012 14:48:05		NT06	Data v lokacích v pořádku	Počet lokací: 1
✓	31.1.2012 10:31:33		NT10	Data v lokacích v pořádku	Počet lokací: 1

Hledat

Hledat v: Vše

Strana: 1 / 1



Závěr

- Moderní technologie musí poskytovat automatizované hlídání jejich zranitelností
- Požadujte sledování zranitelnosti ve všech částech provozovaného IS
- Při automatizovaném sledování zranitelností je možné omezit provádění externích penetračních testů
- Aktivní ISMS v organizaci je velkou výhodou

SECURITY 2012

20. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Martin HANZAL

SODATSW spol. s r.o.

martin@sodatsw.cz

