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

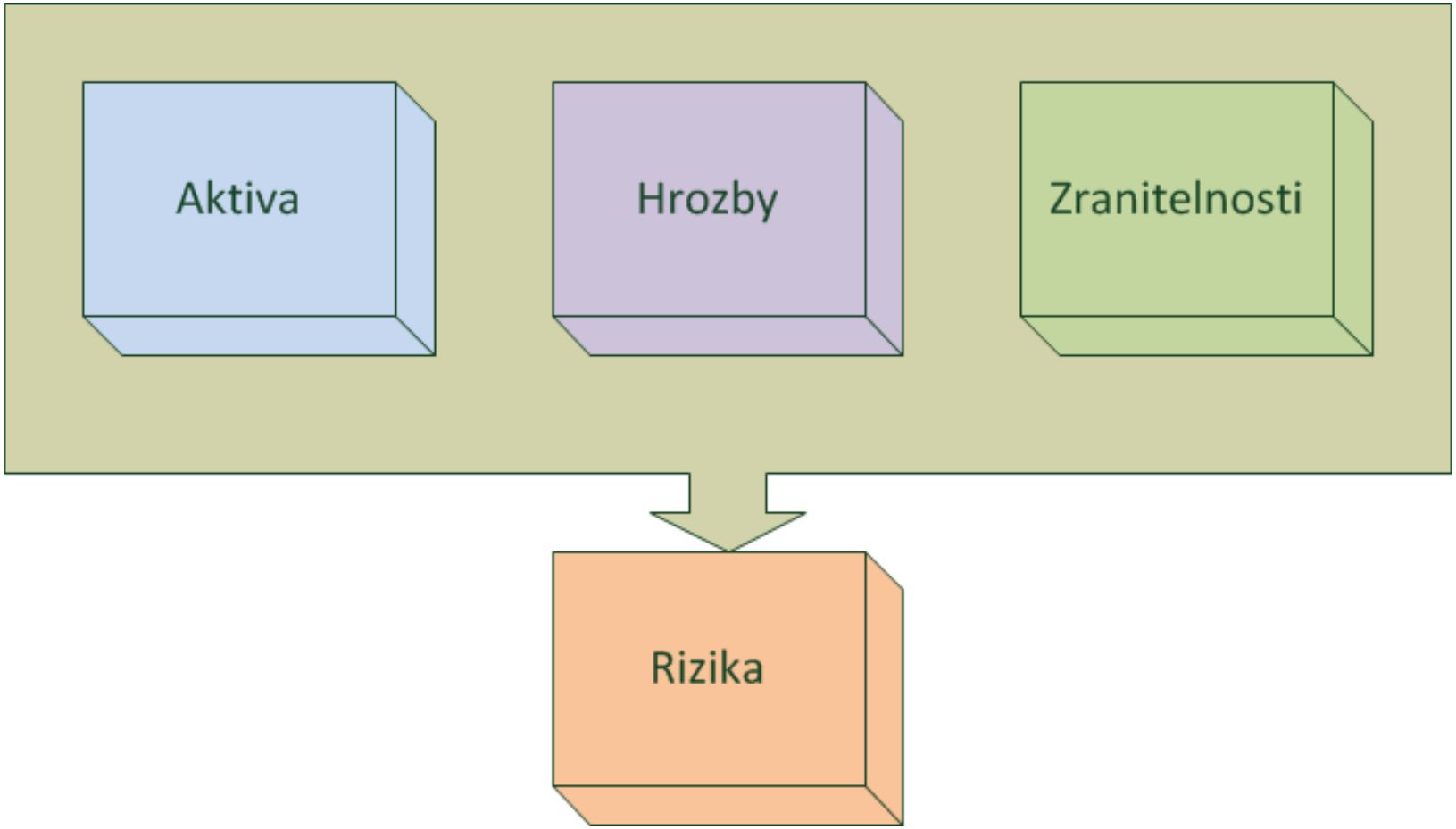
Zranitelnost

- Není to nic nového, řeší se odpradávna
- 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

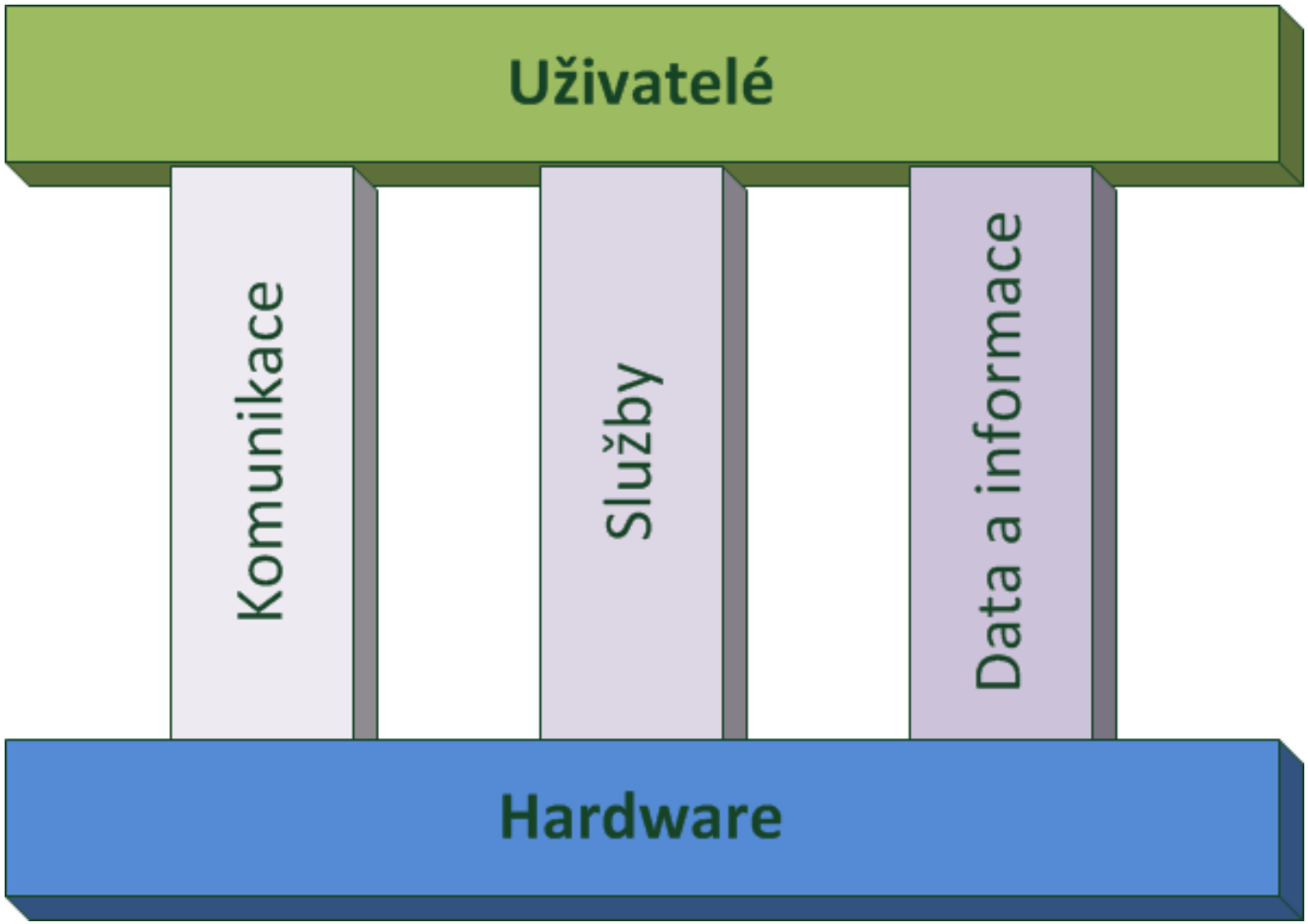
Risk management



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



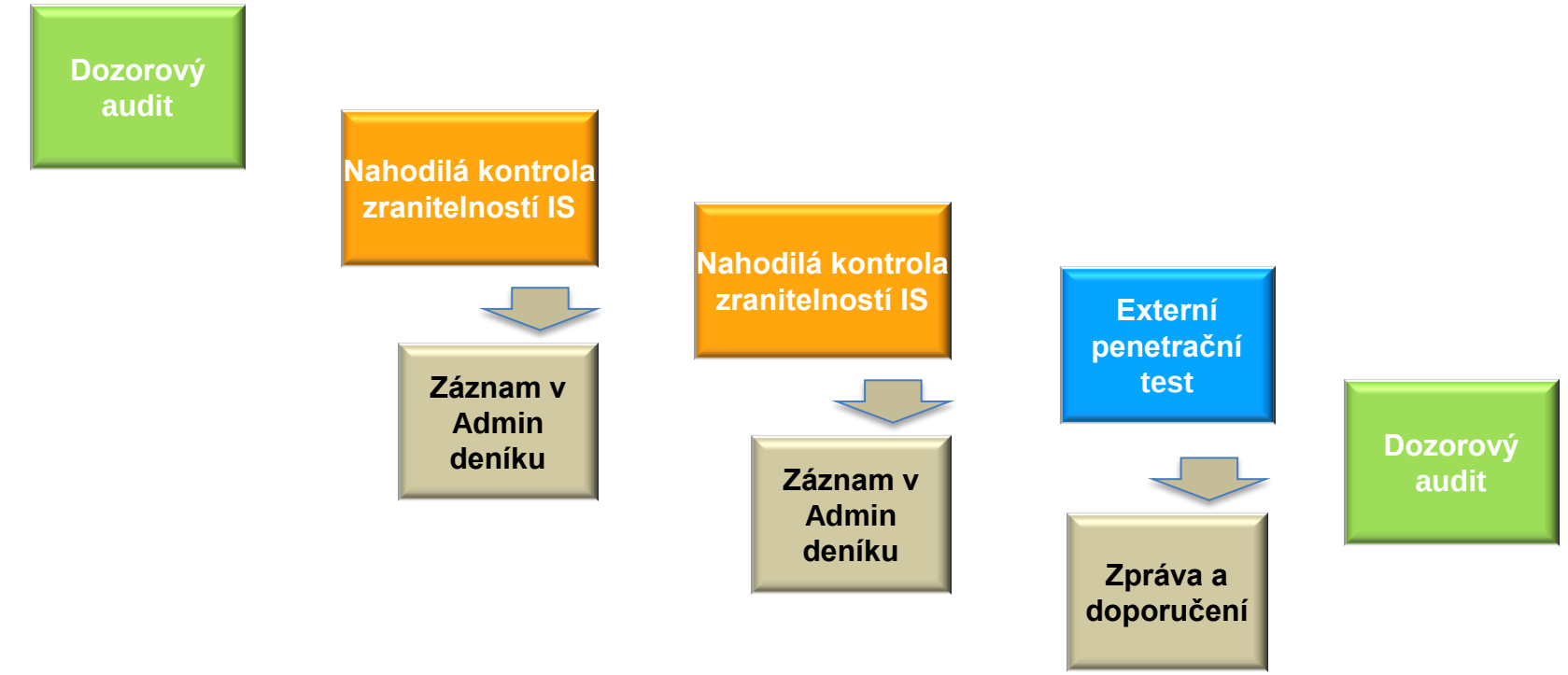
Role řízení zranitelnosti

- 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

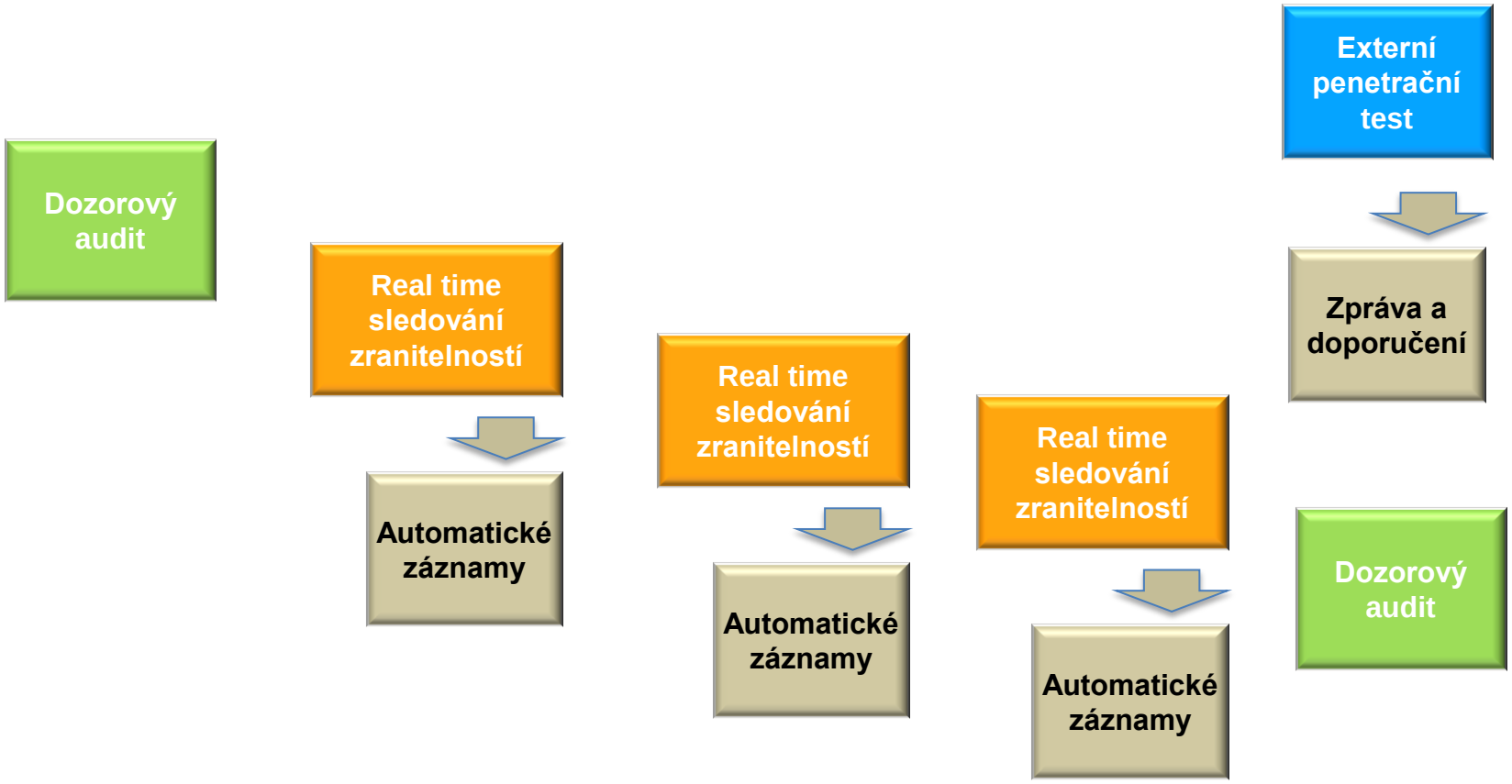
Scénáře řízení zranitelnosti

- 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


Dozorový audit
Real time sledování zranitelností
Automatické záznamy
Real time sledování zranitelností
Automatické záznamy
Real time sledování zranitelností
Automatické záznamy
Externí penetrační test
Zpráva a doporučení
Dozorový audit
1. měsíc
12. měsíc

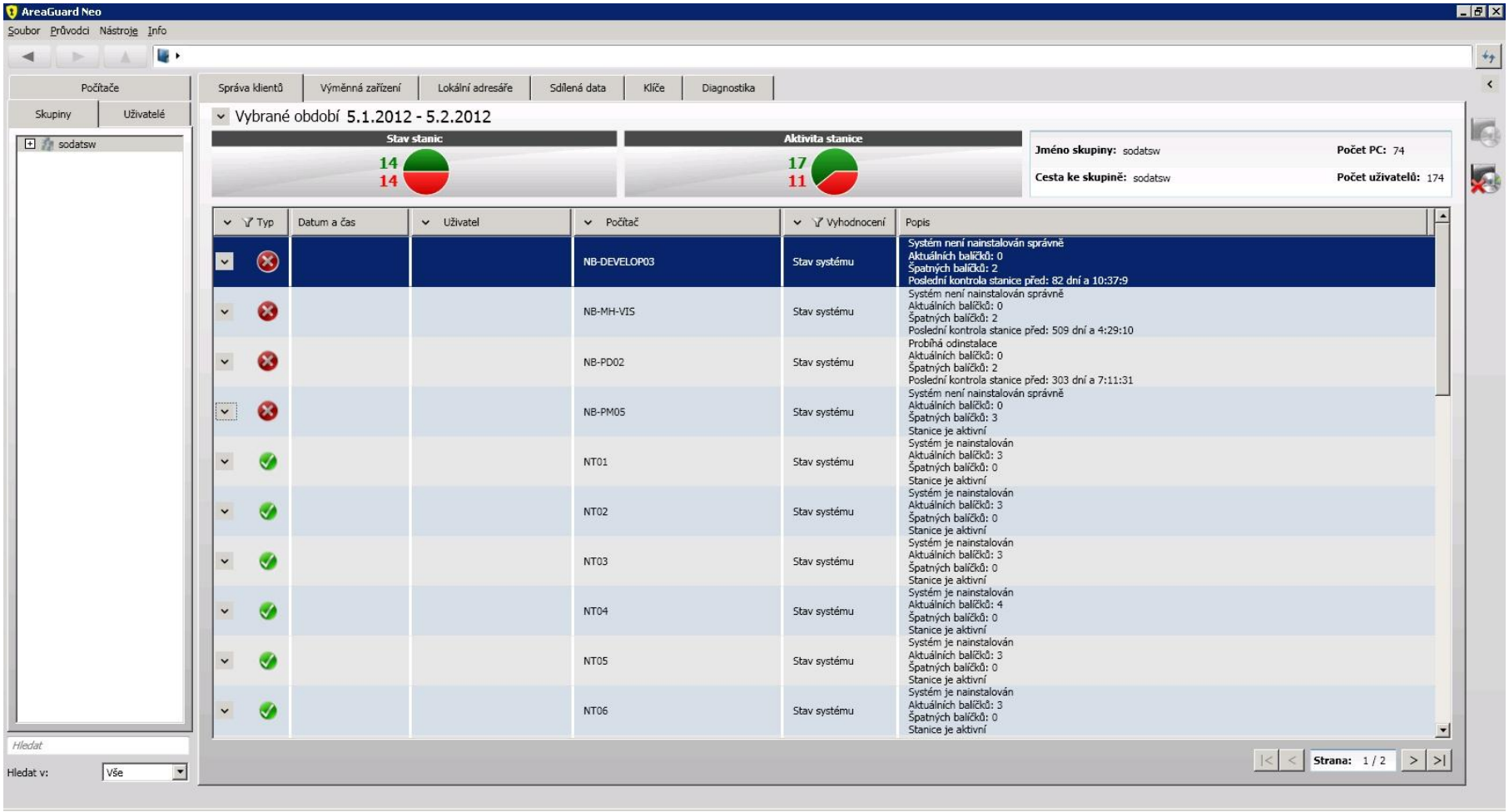
Automatické řízení zranitelnosti

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

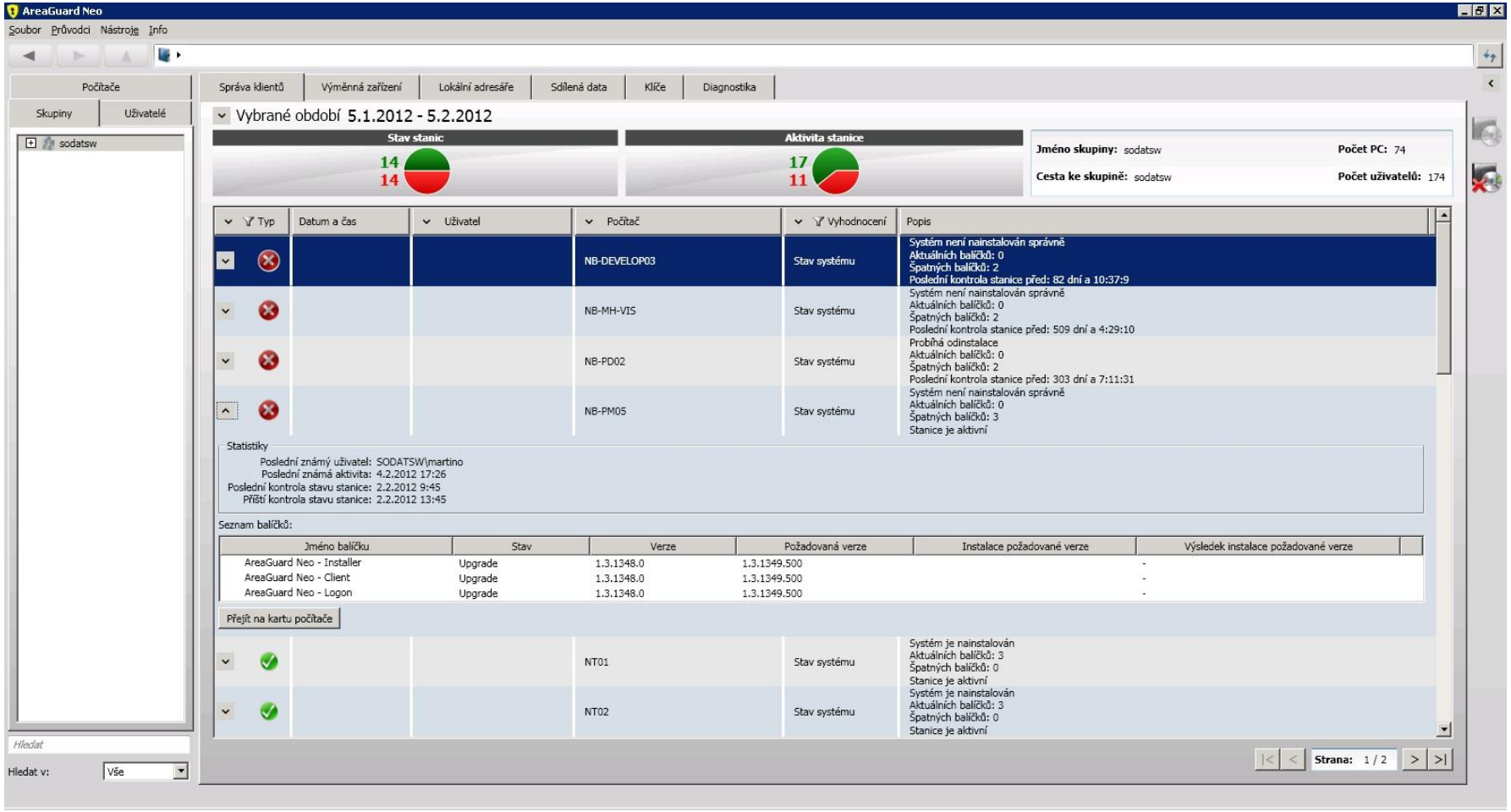
Pokročilé řízení

- 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

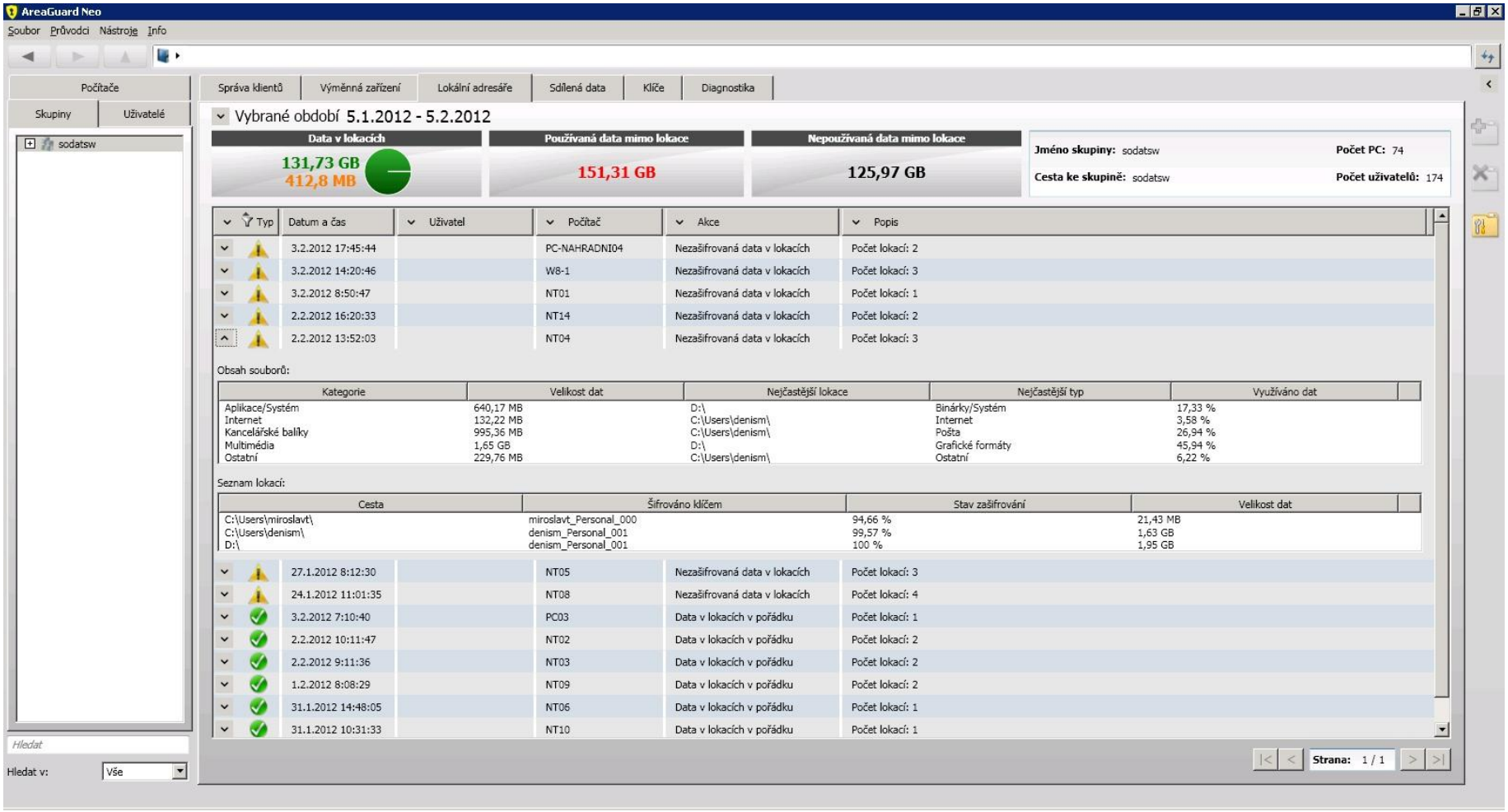
Příklad řízení aktuálních verzí



Příklad řízení aktuálních verzí



Zajištění důvěrnosti dat



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