Att veta eller tro
- Validering av nätverksstrukturen -

Internetdagarna

2005-10-24 – 25

Alf Lundström

Koncerninformationssäkerhetschef

Vattenfall

alf.lundstrom@vattenfall.com

VATTENFALL

Något om Vattenfall

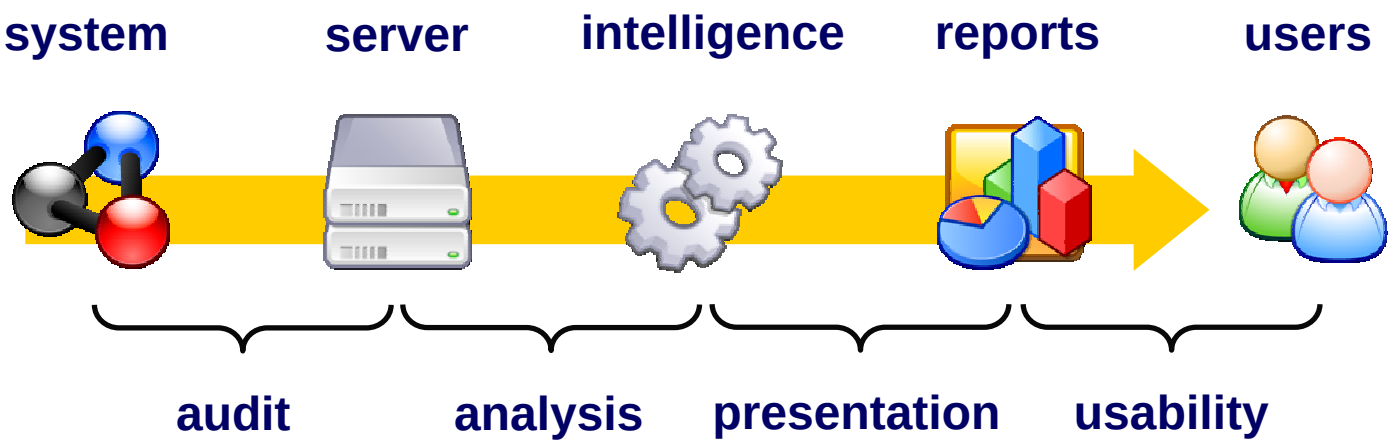
- Ca 37 000 anställda
- I huvudsak verksam i följande länder
  - Sverige
  - Finland
  - Danmark
  - Tyskland
  - Polen
- Ca 32 000 datorer (MS 2000, XP, UNIX)
- Ca 5 000 servrar (MS 2000, 2003, UNIX m fl)
- Stort antal övrig utrustning som routrar, switchar etc

Vattenfall IT Security Scanner

(VITSS)

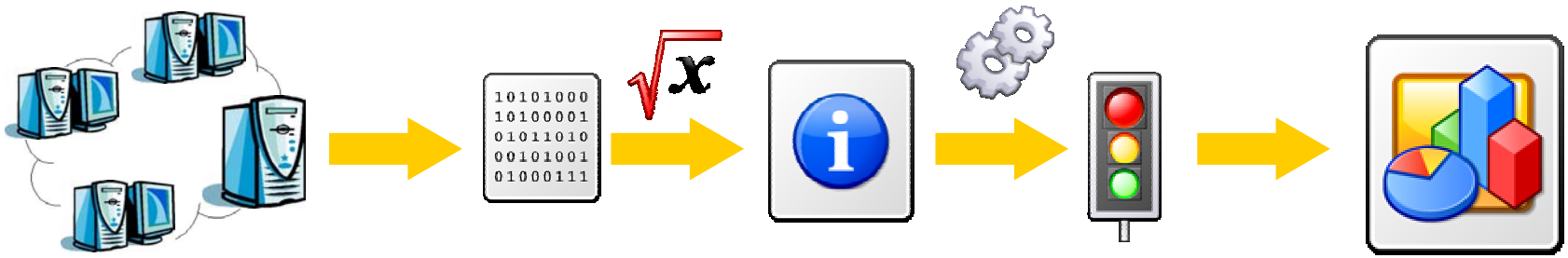
VATTENFALL

Funktionell vy över VITSS



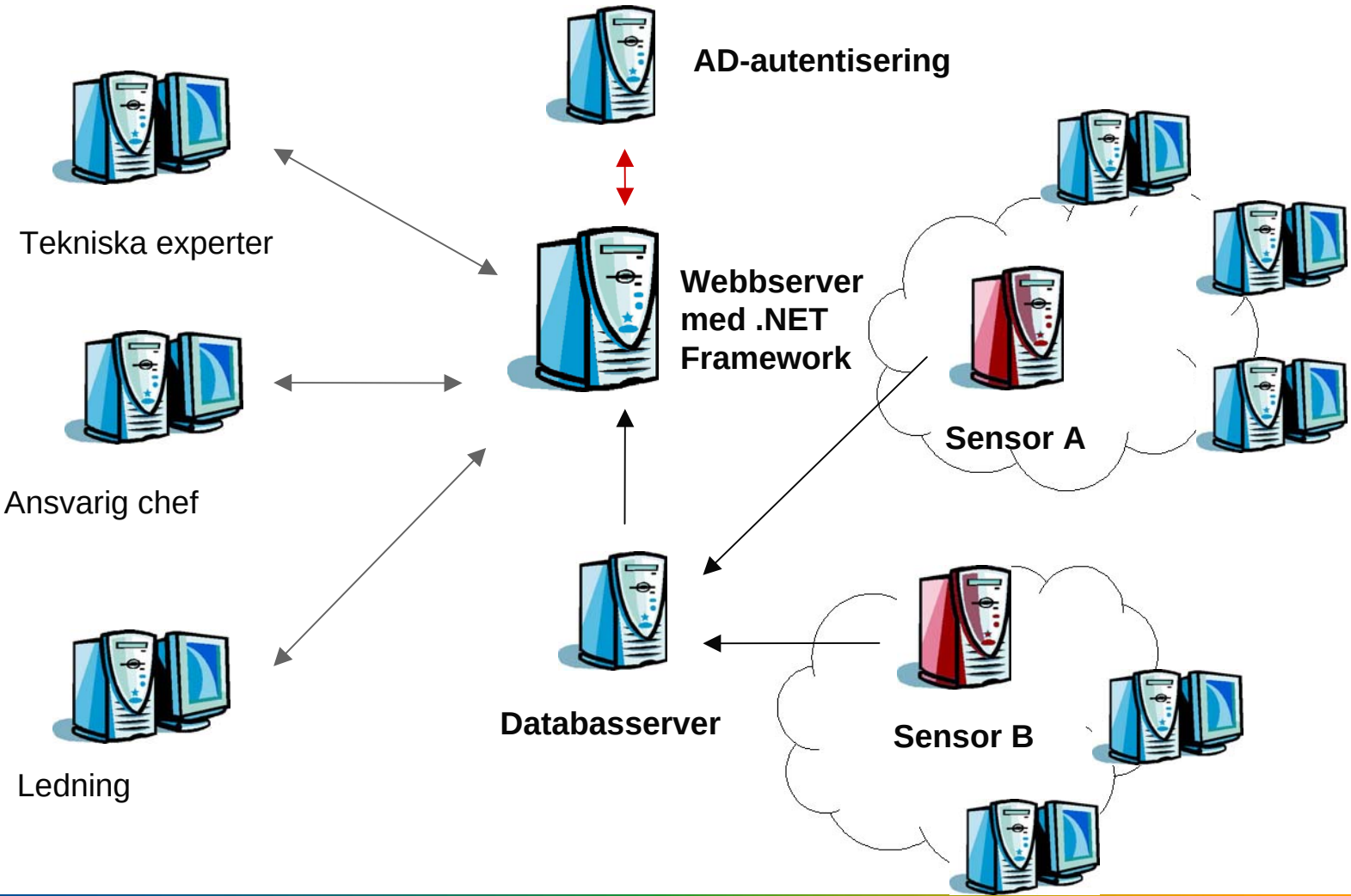
VATTENFALL

Teknisk vy över VITSS (1)



VATTENFALL

Teknisk vy över VITSS (2)



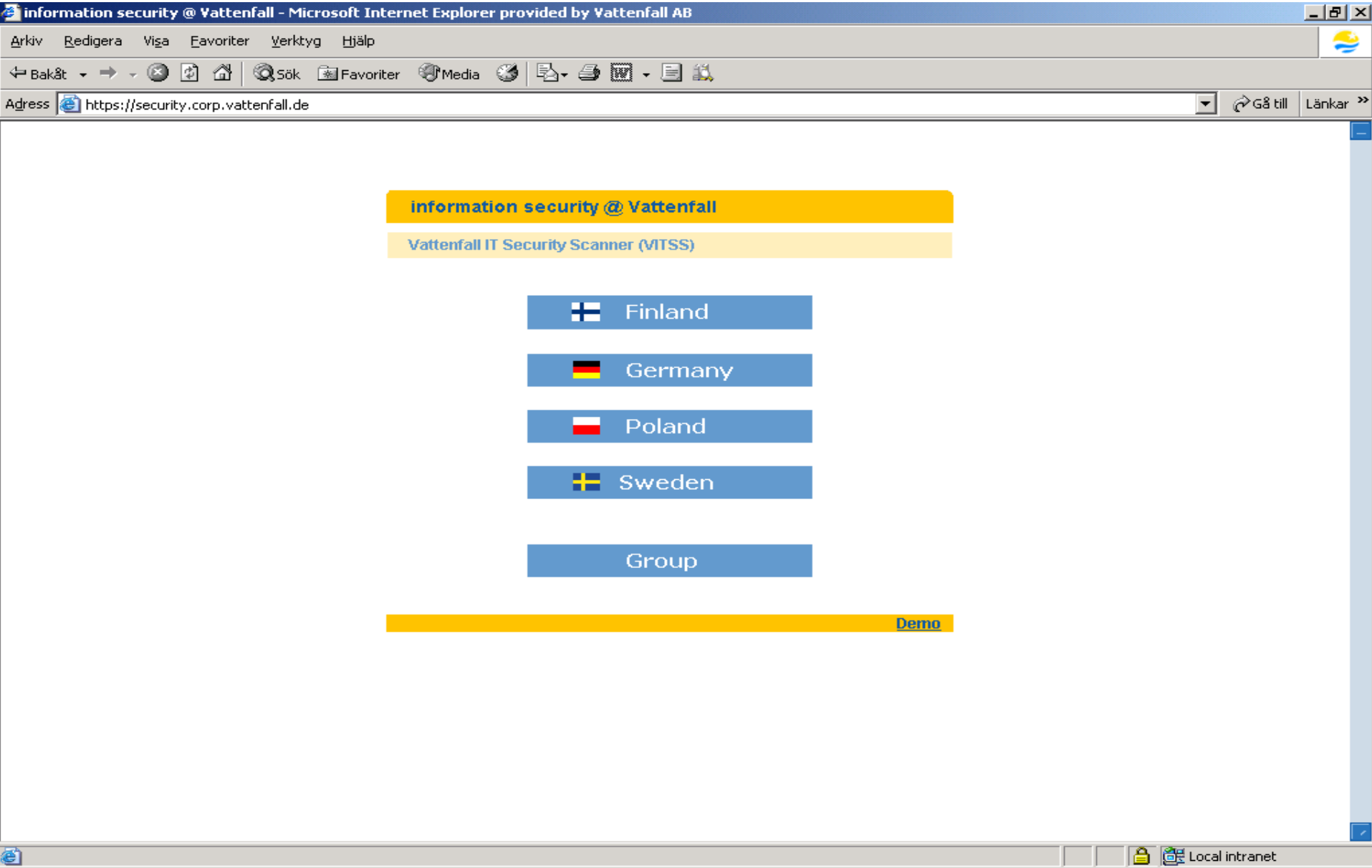
VATTENFALL

Vad ingår i sensordelen?

Skannerdel	Vad som skannas
LanGuard	Windows + windowssäkerhetshål
Nessus	Sårbarheter/säkerhetshål
MBSA	Windows
Jass	Sun Solaris
Hyena	AD, Windows
AV interface	AV software
Tivoli (WMI)	Client, Server
SMS	Windows
Perl Scripts	flexible
nmap	network discov.

- … more coming soon

VATTENFALL


information security @ Vattenfall - Microsoft Internet Explorer provided by Vattenfall AB
Arkiv Redigera Visa Favoriter Verktyg Hjälp
Bakåt Sök Favoriter Media
Adress https://security.corp.vattenfall.de
Gå till Länkar
information security @ Vattenfall
Vattenfall IT Security Scanner (VITSS)
Finland
Germany
Poland
Sweden
Group
Demo
Local intranet

Vattenfall IT Security Scanner - Sweden - Microsoft Internet Explorer provided by Vattenfall AB

Arkiv Redigera Visa Favoriter Verktyg Hjälp

Bakåt Sök Favoriter Media

Adress https://security.corp.vattenfall.de/%5Fsweden/ Gå till Länkar

security @ VATTENFALL

VATTENFALL

general | vulnerabilities | server | client | antivirus | user | management

Welcome to the Vattenfall IT Security Scanner (VITSS)

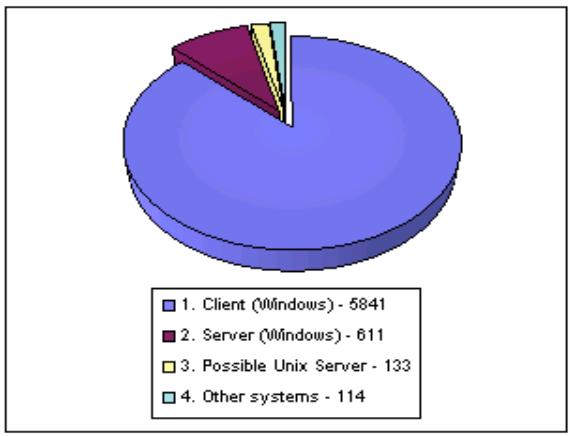
The **Vattenfall IT Security Scanner (VITSS)** is a single point of visibility of the IT security status in the Vattenfall group.

Based on the guidelines of the Vattenfall group (e.g. Group Instruction 26) and the Best Practice (ISO 17799) the target of **VITSS** is

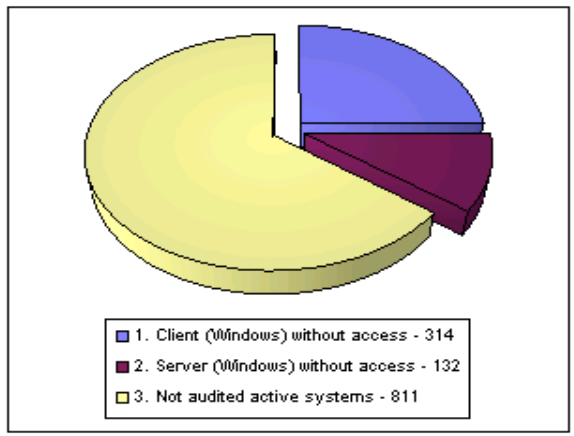
- to identify vulnerabilities and non-compliances of IT systems
- to inventory the IT infrastructure concerning security facts
- to support the risk and threat management with reliable information
- to enable an efficient and measurable minimization of risk
- to control und prioritize actions based on hard technical facts

Current status of the audit

Identificated systems



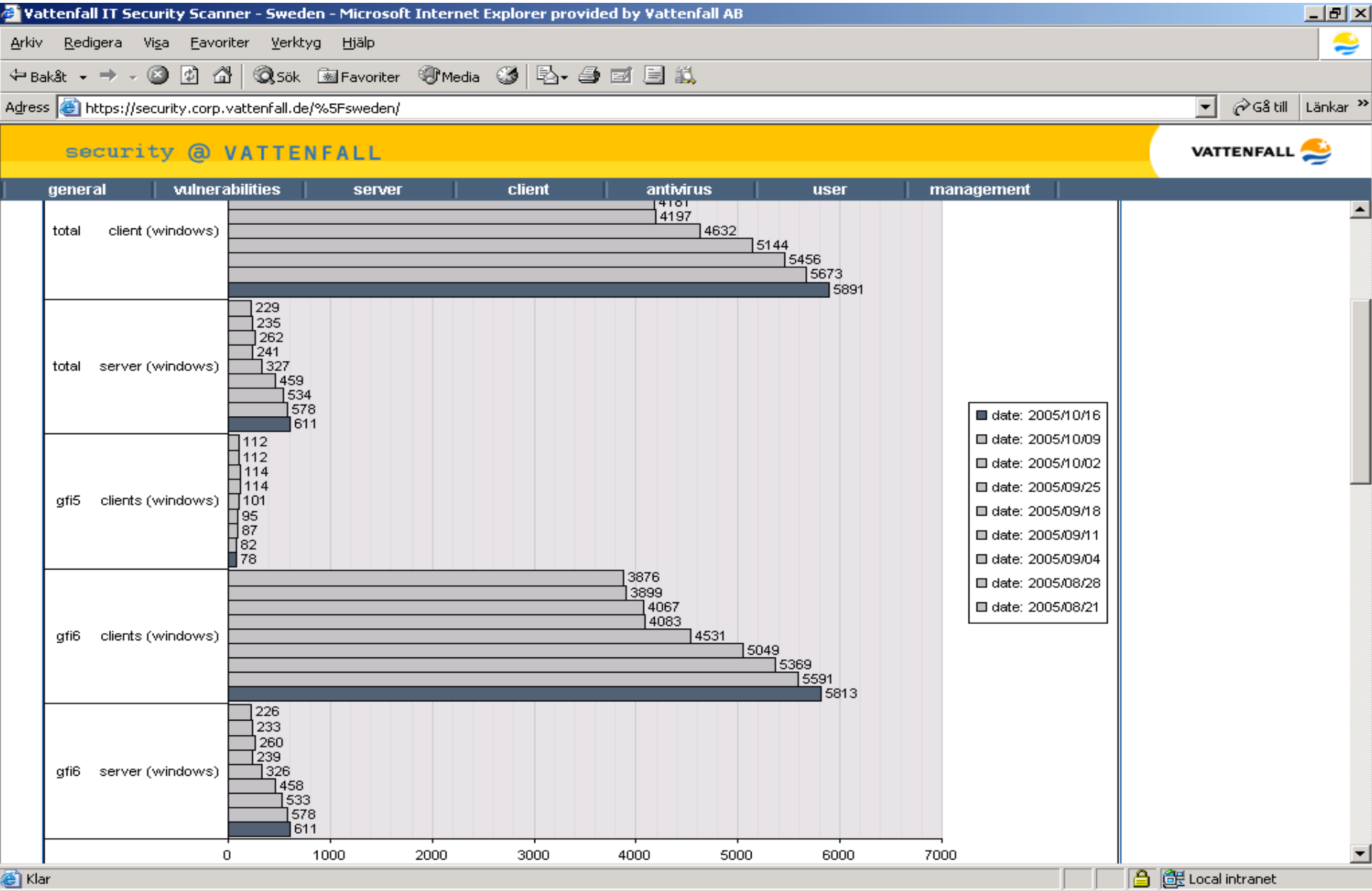
Not audited systems



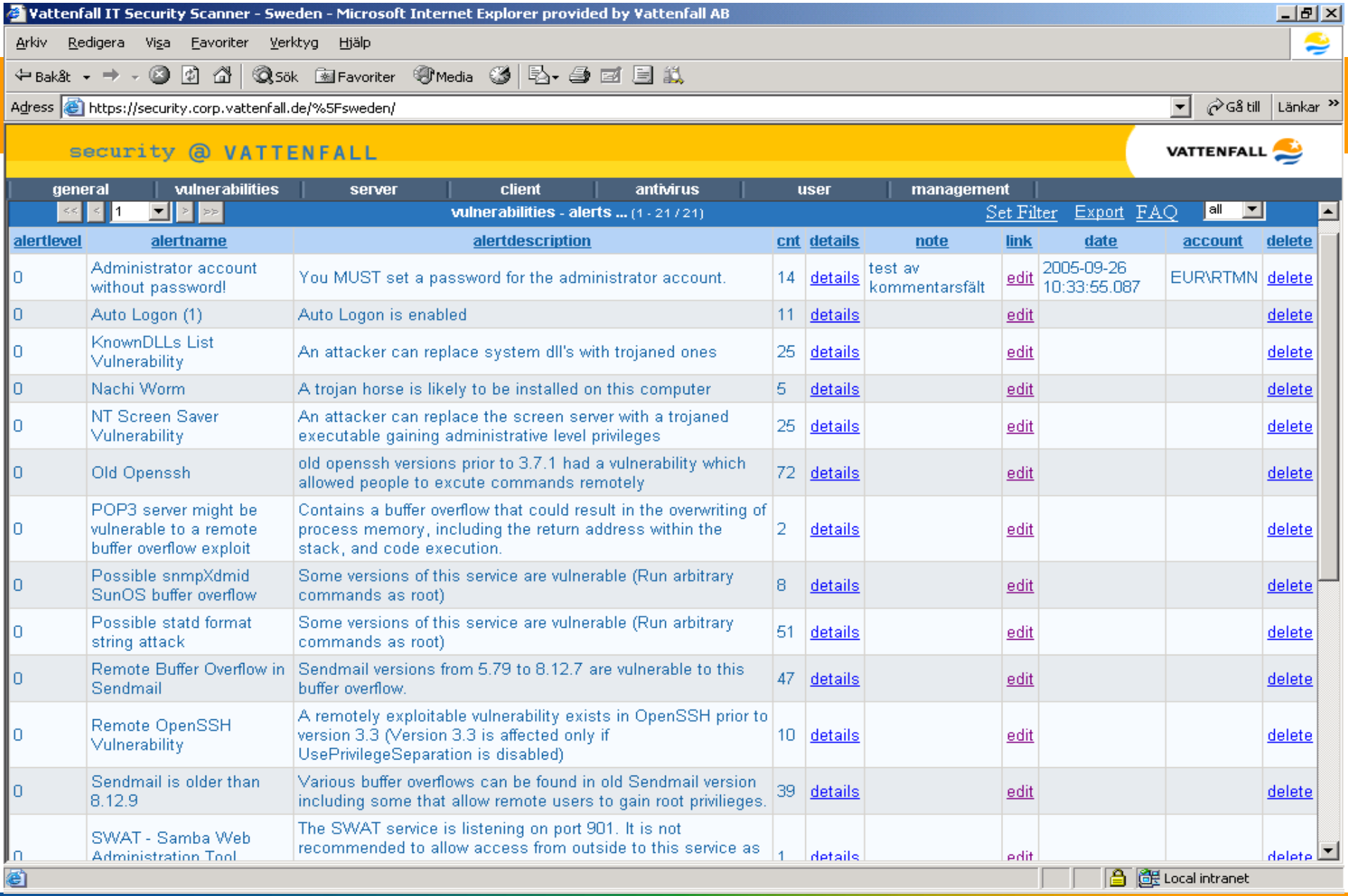
= 7 986

Klar Local intranet

VATTENFALL

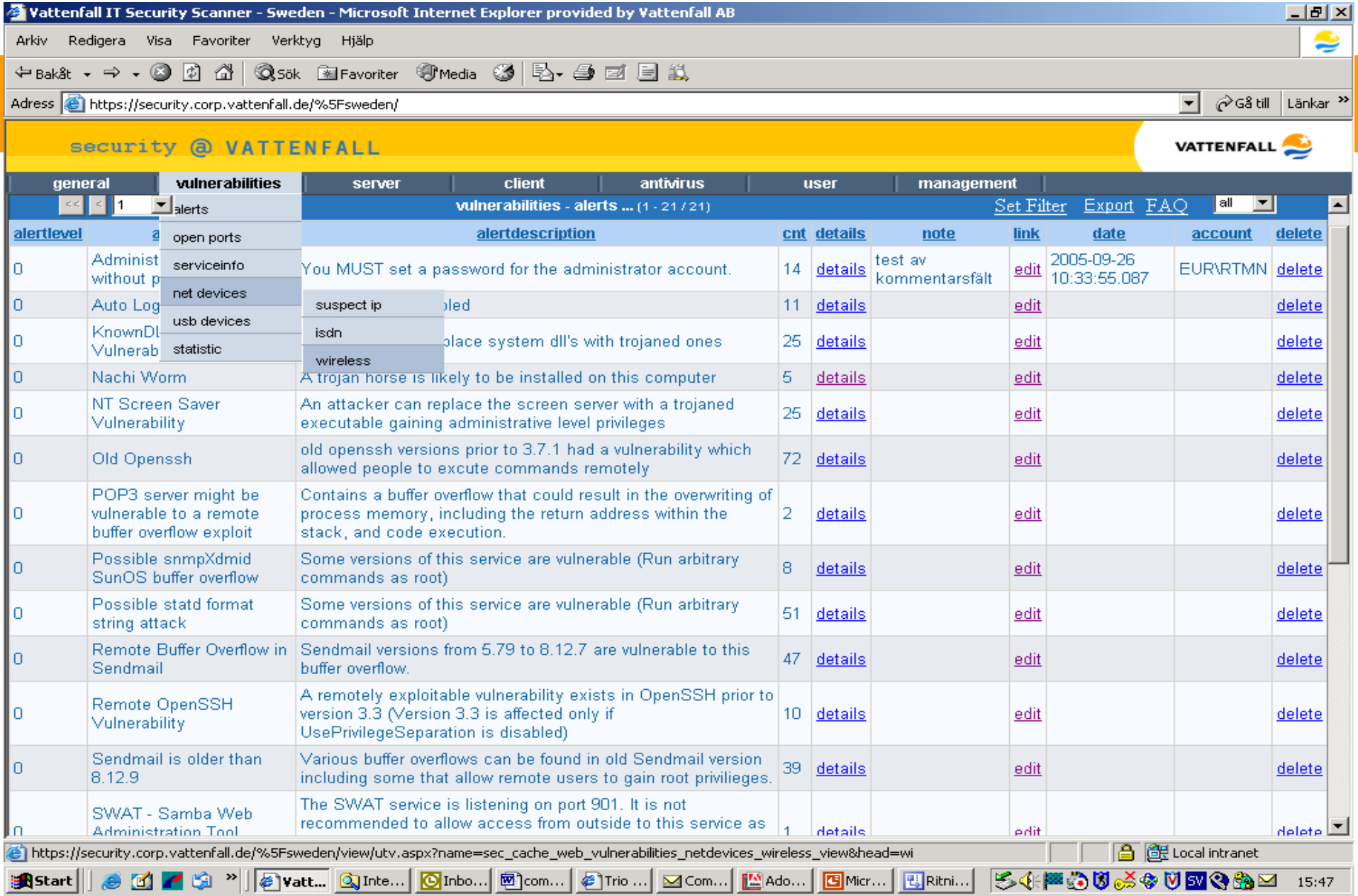


VATTENFALL

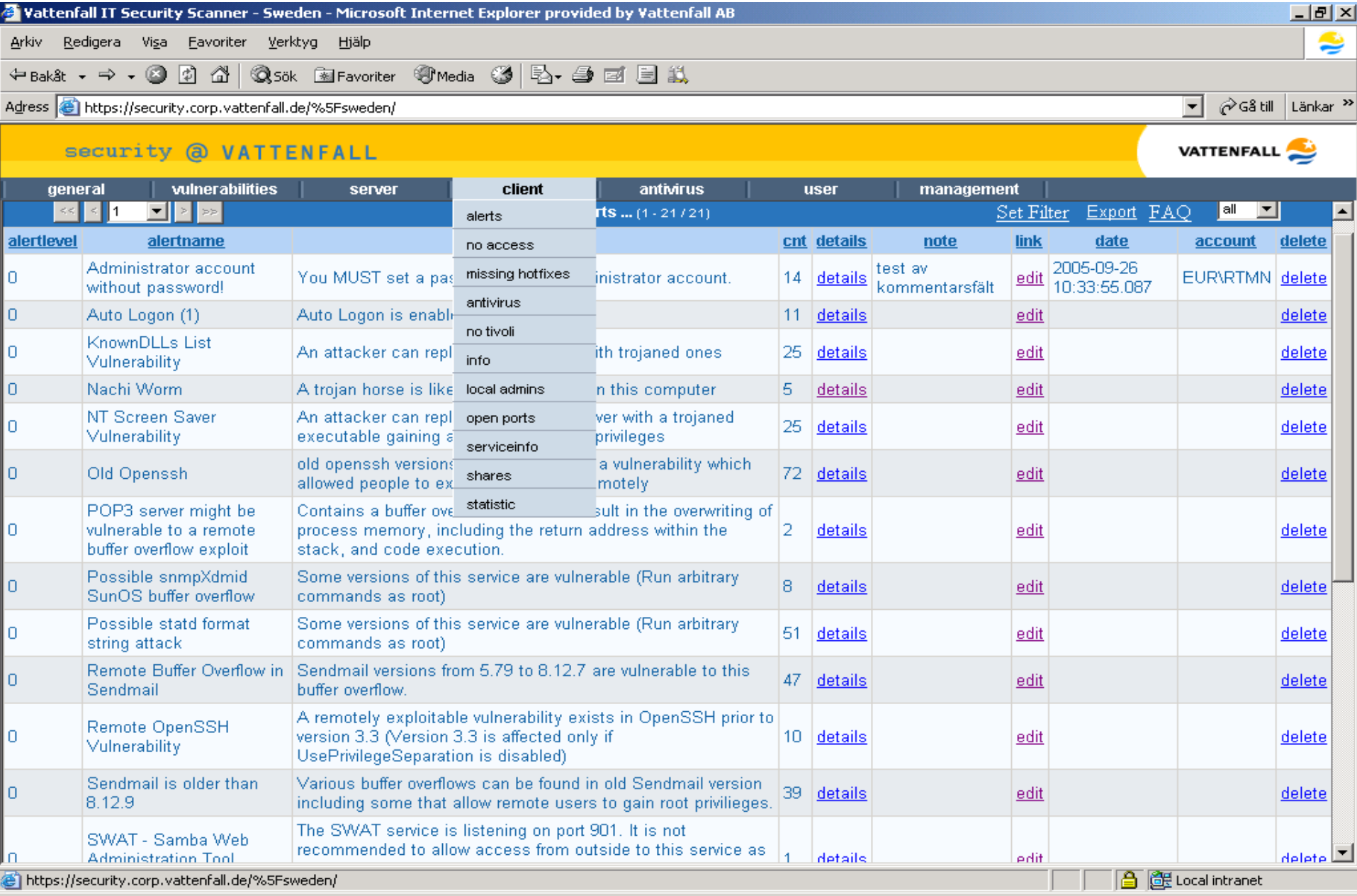


alertlevel	alertname	alertdescription	cnt	details	note	link	date	account	delete
0	Administrator account without password!	You MUST set a password for the administrator account.	14	details	test av kommentarsfält	edit	2005-09-26 10:33:55.087	EUR\RTMN	delete
0	Auto Logon (1)	Auto Logon is enabled	11	details		edit			delete
0	KnownDLLs List Vulnerability	An attacker can replace system dll's with trojaned ones	25	details		edit			delete
0	Nachi Worm	A trojan horse is likely to be installed on this computer	5	details		edit			delete
0	NT Screen Saver Vulnerability	An attacker can replace the screen server with a trojaned executable gaining administrative level privileges	25	details		edit			delete
0	Old Openssh	old openssh versions prior to 3.7.1 had a vulnerability which allowed people to excute commands remotely	72	details		edit			delete
0	POP3 server might be vulnerable to a remote buffer overflow exploit	Contains a buffer overflow that could result in the overwriting of process memory, including the return address within the stack, and code execution.	2	details		edit			delete
0	Possible snmpXdmid SunOS buffer overflow	Some versions of this service are vulnerable (Run arbitrary commands as root)	8	details		edit			delete
0	Possible statd format string attack	Some versions of this service are vulnerable (Run arbitrary commands as root)	51	details		edit			delete
0	Remote Buffer Overflow in Sendmail	Sendmail versions from 5.79 to 8.12.7 are vulnerable to this buffer overflow.	47	details		edit			delete
0	Remote OpenSSH Vulnerability	A remotely exploitable vulnerability exists in OpenSSH prior to version 3.3 (Version 3.3 is affected only if UsePrivilegeSeparation is disabled)	10	details		edit			delete
0	Sendmail is older than 8.12.9	Various buffer overflows can be found in old Sendmail version including some that allow remote users to gain root privilieges.	39	details		edit			delete
0	SWAT - Samba Web Administration Tool	The SWAT service is listening on port 901. It is not recommended to allow access from outside to this service as	1	details		edit			delete

VATTENFALL

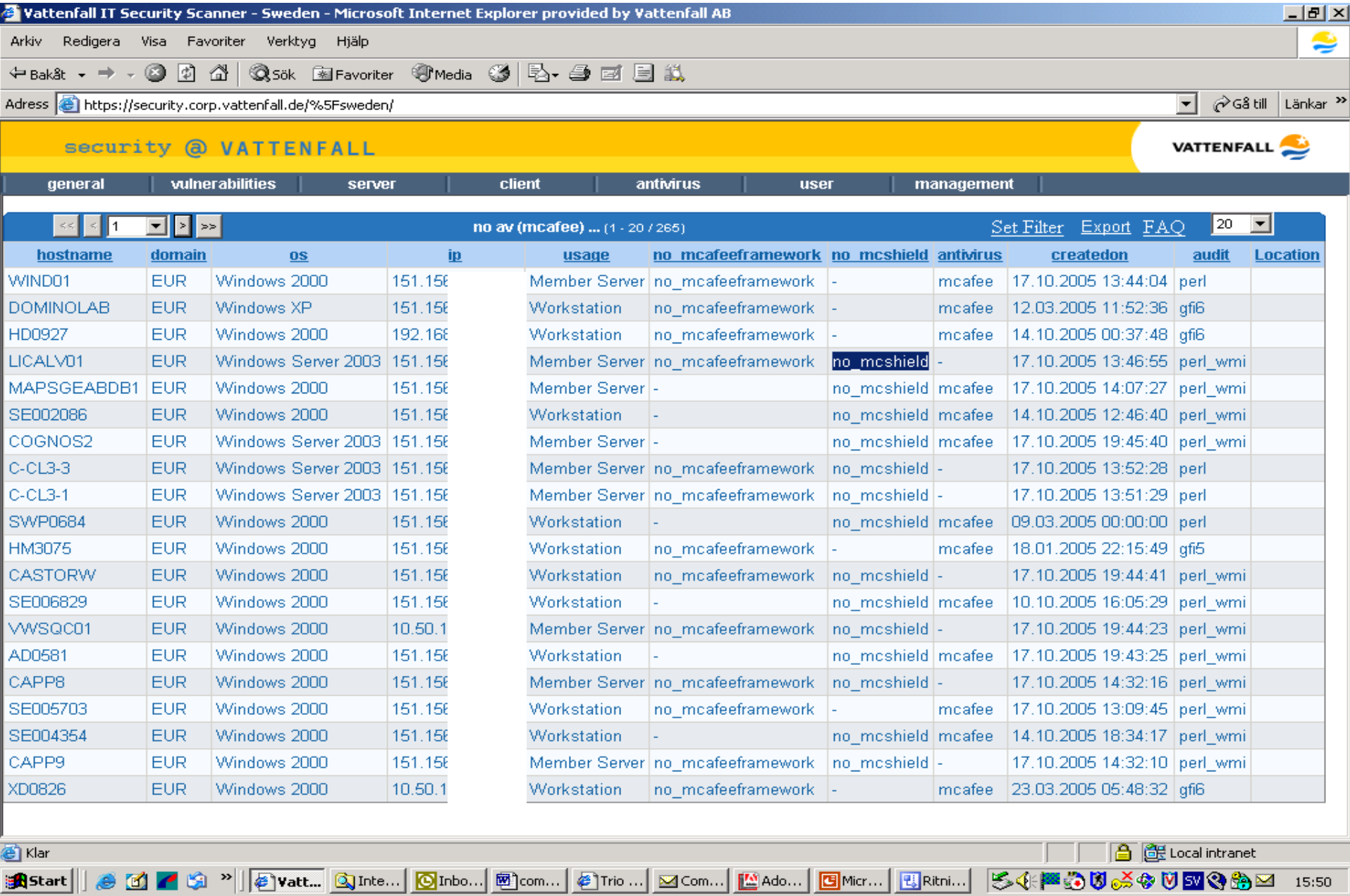


VATTENFALL

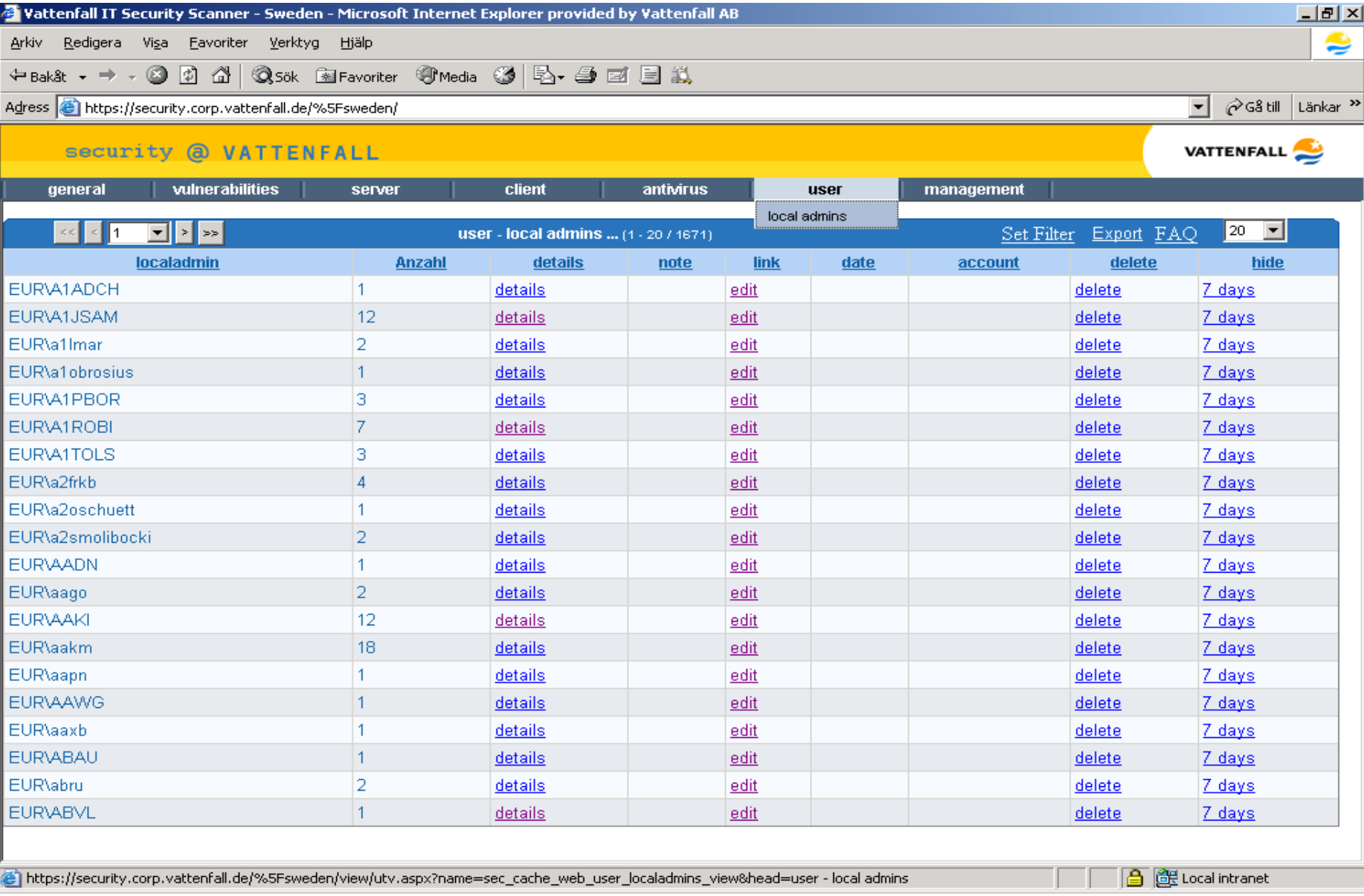


alertlevel	alertname		cnt	details	note	link	date	account	delete
0	Administrator account without password!	You MUST set a pas inistrator account.	14	details	test av kommentarsfält	edit	2005-09-26 10:33:55.087	EUR\RTMN	delete
0	Auto Logon (1)	Auto Logon is enabl	11	details		edit			delete
0	KnownDLLs List Vulnerability	An attacker can repl ith trojaned ones	25	details		edit			delete
0	Nachi Worm	A trojan horse is like n this computer	5	details		edit			delete
0	NT Screen Saver Vulnerability	An attacker can repl ver with a trojaned executable gaining a privileges	25	details		edit			delete
0	Old Openssh	old openssh versions a vulnerability which allowed people to ex motely	72	details		edit			delete
0	POP3 server might be vulnerable to a remote buffer overflow exploit	Contains a buffer ove sult in the overwriting of process memory, including the return address within the stack, and code execution.	2	details		edit			delete
0	Possible snmpXdmid SunOS buffer overflow	Some versions of this service are vulnerable (Run arbitrary commands as root)	8	details		edit			delete
0	Possible statd format string attack	Some versions of this service are vulnerable (Run arbitrary commands as root)	51	details		edit			delete
0	Remote Buffer Overflow in Sendmail	Sendmail versions from 5.79 to 8.12.7 are vulnerable to this buffer overflow.	47	details		edit			delete
0	Remote OpenSSH Vulnerability	A remotely exploitable vulnerability exists in OpenSSH prior to version 3.3 (Version 3.3 is affected only if UsePrivilegeSeparation is disabled)	10	details		edit			delete
0	Sendmail is older than 8.12.9	Various buffer overflows can be found in old Sendmail version including some that allow remote users to gain root privilieges.	39	details		edit			delete
0	SWAT - Samba Web Administration Tool	The SWAT service is listening on port 901. It is not recommended to allow access from outside to this service as	1	details		edit			delete

VATTENFALL



VATTENFALL



localadmin	Anzahl	details	note	link	date	account	delete	hide
EUR\A1ADCH	1	details		edit			delete	7 days
EUR\A1JSAM	12	details		edit			delete	7 days
EUR\a1lmar	2	details		edit			delete	7 days
EUR\a1obrosius	1	details		edit			delete	7 days
EUR\A1PBOR	3	details		edit			delete	7 days
EUR\A1ROBI	7	details		edit			delete	7 days
EUR\A1TOLS	3	details		edit			delete	7 days
EUR\a2frkb	4	details		edit			delete	7 days
EUR\a2oschuett	1	details		edit			delete	7 days
EUR\a2smolibocki	2	details		edit			delete	7 days
EUR\AADN	1	details		edit			delete	7 days
EUR\aago	2	details		edit			delete	7 days
EUR\AAKI	12	details		edit			delete	7 days
EUR\aakm	18	details		edit			delete	7 days
EUR\aapn	1	details		edit			delete	7 days
EUR\AAWG	1	details		edit			delete	7 days
EUR\aaxb	1	details		edit			delete	7 days
EUR\ABAU	1	details		edit			delete	7 days
EUR\abru	2	details		edit			delete	7 days
EUR\ABVL	1	details		edit			delete	7 days

VATTENFALL

Framtida utveckling

- Anpassning till gällande krav, policies, standarder etc
  - GI 26 – Vattenfalls Group Instruction ”Informationssäkerhet”
  - ISO/IEC 1 77 99
  - BASEL 2
  - KontaG
  - PCI
  - etc

- Fortsatt teknisk utveckling
  - Nya tester
  - Bättre integrering mot andra databaser: inventariesystem, personalregister
  - Bättre integrering mot andra säkerhetssystem: informationsklassnings-databas, andra skanningsverktyg

Erhållen information

- Teknisk information
  - Tekniska brister och svagheter
  - ”TODO”-listor till IT-operation
    - Viktigt med information och förståelse för att åtgärda de anmärkningar och avvikelser som framkommit i VITSS

- ”Överskottsinformation”
  - Personliga oegentligheter t ex nedladdning av program och funktioner som strider mot företagets policy och regelverk
    - Rutiner måste finnas och vara avstämda med personal-organisationer m fl, hur denna information får hanteras och av vem.

Avslutning !

VATTENFALL