

Introduction to DK- CERT Vulnerability Database

By Peter Rickers and Mikael Stamm

Fundamental Idea

- Securing of networks, in-house and externally
- Savings for the costumers
- Making admission to the correct information more effective
- Maximum utilization of resources

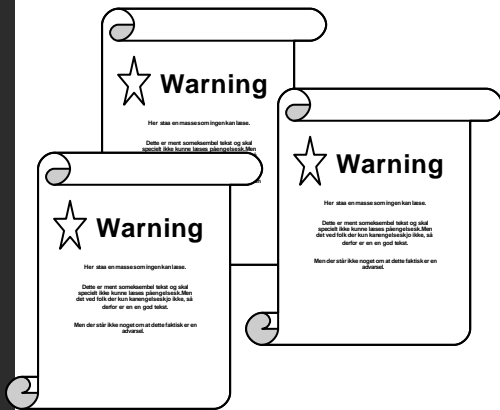
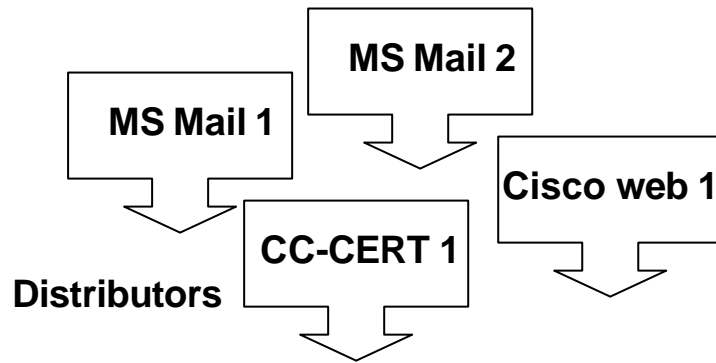
Target Group

- The data base has primarily been constructed for the Danish Research Net, but suitable for the Danish School Net (Sector Net), government institutions, and certain private sector.
- 4500 potential costumers.

Overview

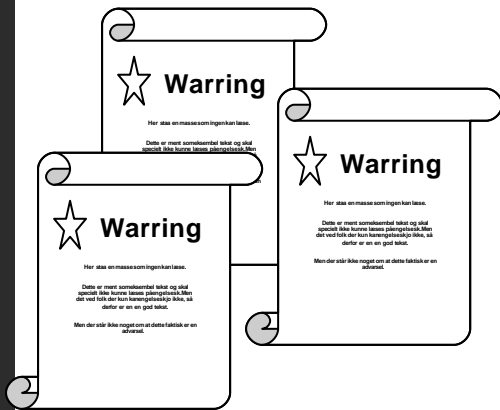
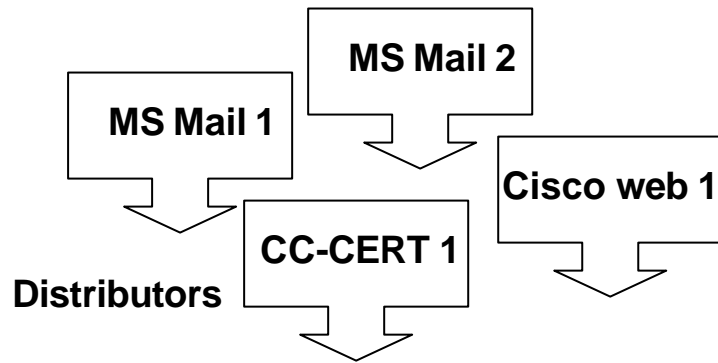
- Basic concepts
- Administrating the system
- From the users point of view

Basic Concepts

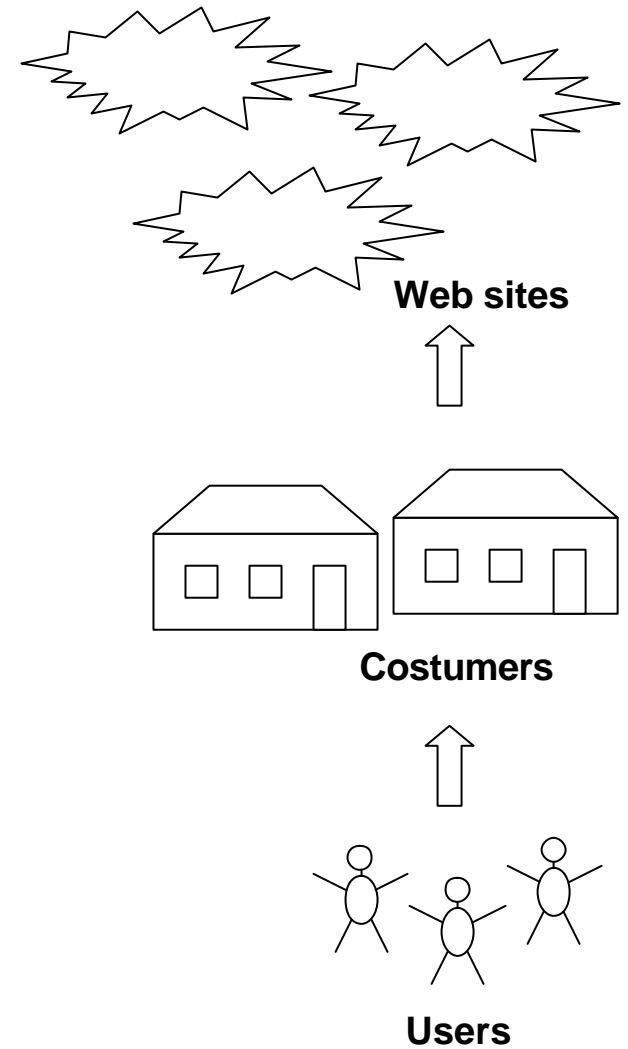


Advisories

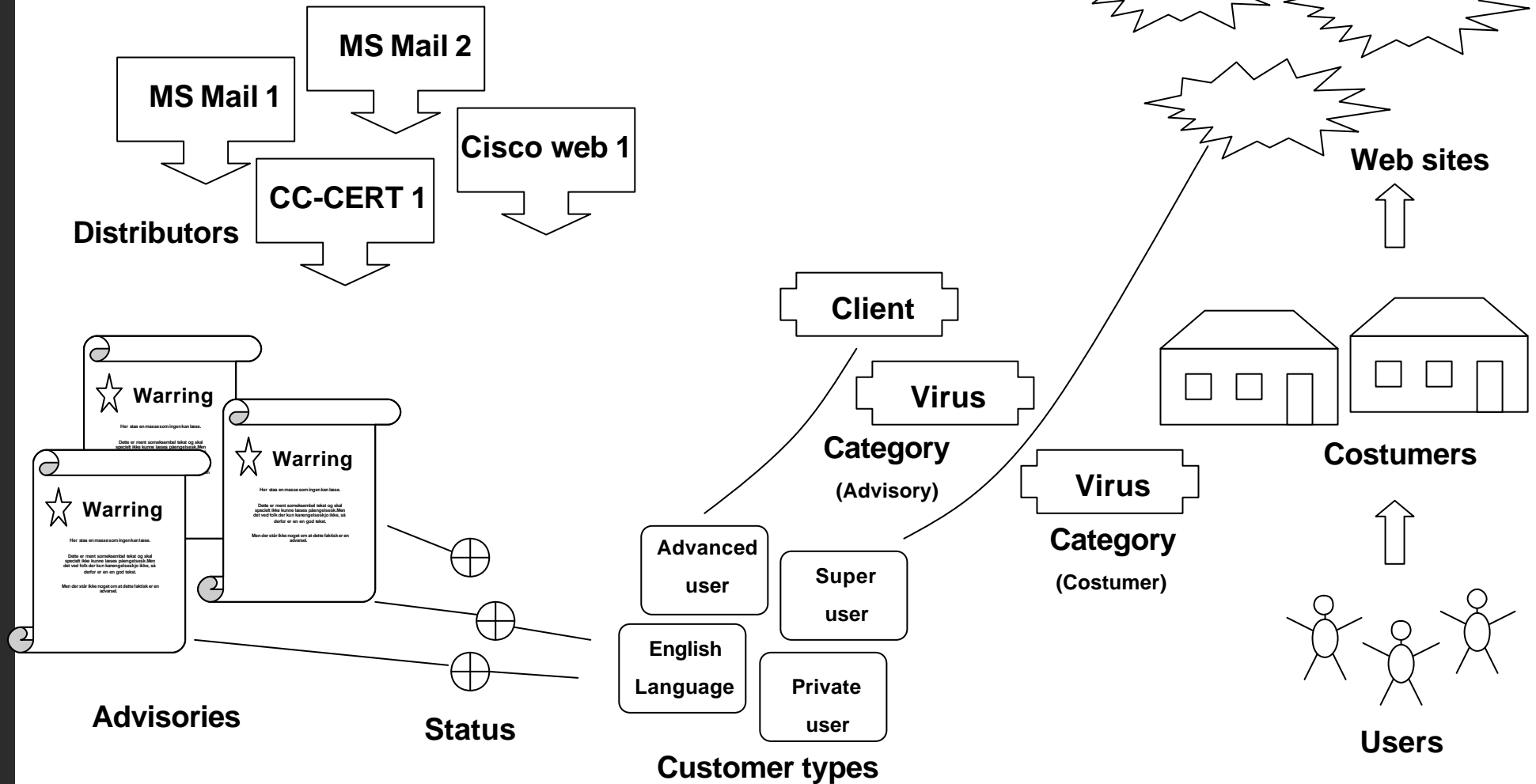
Basic Concepts



Advisories



Basic Concepts



The Administration System

- Advisories administration
 - Edit contents
 - Categorize
 - Control appearance on site
- Customers administration
 - General preferences
 - Categorize
 - Users administration

Contents of an Advisory

- New advisories from
 - mail
 - web harvest
 - staff
- Title/description pr type
- Damage level, date
- Links

The screenshot shows a Microsoft Internet Explorer browser window displaying a web form titled "Advarsler - rediger efter type". The form is used for editing advisories. The main content area shows a preview of an advisory with the following details:

- 0000-00-00 Unparsed - from 'ISS Customer Relations <cbp@iss.net>' - subject '[Xpress] Internet Scanner X-Press Update 6.10 is Now Available!'**
- Titel:** engelsk (selected), Brug Default, Default
- Beskrivelse:** Internet Scanner X-Press Update 6.10 is now available from the ISS. Download Center: <http://www.iss.net/download/>. Internet Scanner XPU 6.10 contains 24 new checks and fixes for 16 existing checks. XPU 6.10 focuses on Oracle Application Server and Windows XP. PROTECTION BENEFITS: Operating Environment.
- Dato:** 0000-00-00 (Datoformat: 8888-mm-dd)
- Vurdering:** Lav
- CVE/CAN:** 0000-0000
- Links:** Ny, Rediger, Slet, Åben
- Vejledning:** GEM: Gem den nye advarsel. TILBAGE: Tilbage til oversigt over advarsler.

The form includes buttons for "Gem" (Save) and "Annuller" (Cancel). The browser's address bar shows the URL: <http://c2dkt.vhostip2.hugin6.webhotel.net.uni-c.dk/per/adminsystem/AdminSystemResult.cgi>.

Category for an Advisory

- Bunch of masks
 - Main group
 - Ex: Server software
 - OS info
 - Ex: Windows, 2000, *
 - App. Info
 - Ex: Exchange server, 2000, *

Advarsler - Aktuelle kategorier - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://c2dkt.vhostip2.hugin6.webhotel.net.uni-c.dk/perl/adminsystem/AdminSystemResult.cgi?action=AdvisoryMaskEditList&aid=360

Links O'Reilly Zvon XSL Tutorial Vltlisten! UserFriendly Dilbert Bugzilla WG META FAQ CERT Bugzilla CVS Book ASCII - ISO 8859-1 Table with HTML Entity Names

Advarsler
Aktuelle kategorier

0000-00-00 Unparsed - from 'ISS Customer Relations' - subject '[Xpress] Internet Scanner X-Press Update 6.10 is Now Available!'

[N] Virus/Windows/**/Microsoft Exchange/**

Ny
Kopier
Slet
Fortryd ret
Gem

Forrige Næste Annuller

Hovedkategori

Operativsystem
PreEdit
Serverprogrammel
Sikker kommunikation
Virus

Operativsystem

Type	Version	Patch
Ulrix	*	*
Unisis	2000	
UnixWare	2000 Advanced Server	
VMS	2000 Datacenter Server	
Windows	2000 Professionel	
Wlrex Immunix OS	2000 Server	

Applikation

Navn	Version	Patch
Microsoft Acces	*	*
Microsoft DNS Server	2000	
Microsoft Excel	5.5	
Microsoft Exchange		
Microsoft FrontPage Server		
Microsoft Frontpage		

Føj til liste

Done Internet

Status for an Advisory

- Represent “life cycle” of the advisory
 - New advisory
 - Still in preparation
 - Ready – but not approved
 - Online on site
- Status for each customer type

Customer

- Defines users view on the system
 - Type – information “language”
 - Site – general layout
- Customer groups
 - Overview in the administration system
- Users – interaction with the system
- Categories – reflects interest areas

Users

- Users have the following information:
 - Username and password
 - Name and title
 - Email and mobile phone number
- Provide
 - Login to the web interface
 - Notification messages from the system

The System from the Users Point of View

- Private area on the website for each customer
- Menu for changing own preferences.
- Navigation in the advisories – based on own categories (interest areas)
- Advisories ...

Velkommen til DK•CERTs sikkerhedsprodukt - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites History Print Mail

Address <http://c2dkt.vhostip2.hugin6.webhotel.net.uni-c.dk/perlc/customerSystem/OutputSystem.cgi?action=ShowPage&template=templates/CustomerSystem/frontpage.html> Go

Links O'Reilly Zvon XSL Tutorial Vitslisten! UserFriendly Dilbert Bugzilla WG META FAQ CERT Bugzilla CVS Book

DK•CERT

Danish Computer Emergency Response Team FORSIDE | LOGIN SOM SYSTEMEJER | NYHEDER | ARTIKLER | VEJLEDNINGER | KONTAKT | ANMELD | OVERSIGT

Demo Customer

System Developer Peter Rickers

Seneste ændringer i produktlisten: 22/05-2002 kl. 17:59:51

NYHEDER

Nyhed fra UNI•C
Alt er fint !! ▶

Et større antal servere i Danmark er blevet hacket
Et større antal servere i Danmark er de seneste døgn blevet hacket af uvedkommende ved udnyttelse af kendte sårbarheder i SSH. ▶

Gone(r) virus/orrm
Der er konstateret en ny orm og den ses i stort antal i Danmark. Ormen er meget destruktiv, da den aktivt søger efter en mængde programmer - af sikkerhedsmæssig karakter - og sletter dem, for selv at få frit råderum. ▶

BadTrans Virus/Orrm
Denne virus er en e-mail-orm, der tilsyneladende rammer danskere i stort omfang. Den anretter, så vidt vides i skrivende stund, ikke skade på data på inficerede systemer, men kan til gengæld smitte maskiner åbne for en ældre MIME-sårbarhed. ▶

Flere nyheder ... ▶

ABONNEMENTSYDELSER

- Seneste sårbarheder ▶
- Rediger indstillinger ▶
- Anmeld en sikkerhedshændelse ▶
- Spørg DK•CERT ▶
- Vejledning til sårbarhedsdatabasen ▶

Internet

Velkommen til DK•CERTs sikkerhedsprodukt - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites History Print Mail

Address utSystem.cgi?action=ShowPage&Main=Serverprogrammel&OS=Windows&Application=MS%20IIS&template=templates%2FCustomerSystem%2Fadvisoriespage.html Go

Links [O'Reilly](#) [Zvon XSL Tutorial](#) [Vitslisten!](#) [UserFriendly](#) [Dilbert](#) [Bugzilla WG](#) [META FAQ](#) [CERT Bugzilla](#) [CVS Book](#)

DK•CERT

Danish Computer Emergency Response Team [FORSIDE](#) | [LOGIN SOM SYSTEMEJER](#) | [NYHEDER](#) | [ARTIKLER](#) | [VEJLEDNINGER](#) | [KONTAKT](#) | [ANMELD](#) | [OVERSIGT](#)

Information for Peter Rickers, Demo Customer [◀ TILBAGE TIL SYSTEMEJER FORSIDE](#)

OPERATIVSYSTEM	APPLIKATION	ADVARSLER
Fortolkere: Windows ▶ Operativsystem: Windows ▶ Serverprogrammel: Windows ▶ Sikker kommunikation: Windows ▶ Virus: Windows ▶	MS IIS ▶ CheckPoint Firewall-1 ▶ Microsoft SQL Server ▶ EFTP ▶ Microsoft Internet Explorer ▶ Ikke angivet ▶ ValiCert Enterprise VA ▶ Microsoft Exchange ▶ Apache ▶ PHP ▶ None ▶ MS Commerce Server ▶ Microsoft XML Core Service ▶ Microsoft Outlook ▶ SNMP ▶ telnet ▶ Interix ▶ iPlanet Webserver ▶ OmniHTTPd ▶ Netscape Webserver ▶ PPTP ▶ SH39 MailServer ▶ Oracle ▶ Cisco CallManager ▶ FTGate Mailserver ▶ Microsoft Office ▶ SQL ▶ FormMail ▶	2002-04-10 MS02-018 Flere sårbarheder i Microsoft IIS ▶ 2002-03-06 IIS returnerer IP adresser i HTTP headeren ▶ 2002-03-06 Sårbarhed i WinNT sikkerheds politik ▶ 2002-02-27 Sårbarheder i PHP program til webservere ▶ 2001-12-22 Sårbarheder i IIS' håndtering af session ID cookies ▶ 2001-05-03 Svaghed i ISAPI Extension for IIS 5.0 Server ▶ Flere advarsler ▶

Internet

Advarsler - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites History Print Mail

Address stip2.hugin6.webhotel.net.uni-c.dk/perl/customersystem/OutputSystem.cgi?action=ShowPage&aid=564&template=templates%2FCustomerSystem%2Fadvisory.html Go

Links O'Reilly Zvon XSL Tutorial Vitslisten! UserFriendly Dilbert Bugzilla WG META FAQ CERT Bugzilla CVS Book

DK•CERT

Danish Computer Emergency Response Team FORSIDE | LOGIN SOM SYSTEMEJER | NYHEDER | ARTIKLER | VEJLEDNINGER | KONTAKT | ANMELD | OVERSIGT

IIS returnerer IP adresser i HTTP headeren

Dato:
2002-03-06

Vurdering:
Mellem

Beskrivelse:
En sårbarhed i IIS medfører, at Current-Location kan angive interne IP adresser, som normalt er gemt eller maskeret bag en Network Address Translation (NAT) Firewall eller proxy server.

Ved brug af statiske HTML sider, fx. Default.htm, tilføjes en Content-Location header til svar på forespørgelser. Som standard i Microsoft Internet Information Server (IIS) angiver Content-Location IP adressen på serveren istedet for hostnavnet eller domænet (FQDN).

IIS 5.x og 4.0 er sårbare, hvis 'Basic authentication' er aktiveret.

Løsning: Microsoft har angivet følgende vejledning til at forhindre afsløring af interne IP adresser:

Microsoft advarer imod forkert brug af Adsutil.vbs filen. Brug af filen er på eget ansvar.

Åbn en kommando prompt og angiv stien til adminscripts (Denne kan være forskellig afhængigt af den enkelte installation): c:\inetpub\adminscripts (IIS 5.x) c:\winnt\system32\inetsrv\adminsamples (IIS 4.0)

Kør kommandoerne: adsutil set w3svc/UseHostName True net stop iisadmin /y net start w3svc

Istedet vil IIS serveren nu bruge en maskines hostnavn.

LINKS

- Beskrivelse af IIS Authentication ▶
- Microsofts beskrivelse af sårbarheden ▶
- Yderligere oplysninger ▶

Done Internet

Kundesystem - Tekniske kontaktpersoner - Microsoft Internet Explorer

Rediger indstillinger

Tekniske kontaktpersoner

Demo Customer

UserID:	<input type="text" value="newpr"/>	Vejledning: Foretag de ønskede ændringer og tryk gem. SMS er en forsøgsordning.
Fornavn:	<input type="text" value="Peter"/>	
Efternavn:	<input type="text" value="Rickers"/>	
Titel:	<input type="text" value="System Developer"/>	
E-mail:	<input type="text" value="Peter.Rickers@uni-c.dk"/>	
Mobiltlf/SMS:	<input type="text" value="22245511"/>	
Nyt password	<input type="text"/>	

Kundesystem - Kategorier - Microsoft Internet Explorer

Rediger indstillinger

Kategorier

Demo Customer

*\Windows*****

\Redhat Linux/7.0 - i586/Samba**

\Redhat Linux/7.0 - i586/Apache/1.3.24*

Ny

Rediger

Kopier

Slet

Tilbage Printervenlig version

Vejledning:

I boksen vises de systemer, der er registreret i databasen, på formen:
Hovedkategori/operativsystem/version/patch/application/version/patch

Patch dækker over såvel patchniveau, servicepack og hotfix.

* bruges, når du ikke ønsker at specificere (*="alt")

Tryk **ny** for at tilføje kategori.
Marker en kategori og tryk **rediger** for at redigere en eksisterende kategori.
Marker en kategori og tryk **kopier** for at oprette en kategori, der er næsten identisk med en eksisterende. Marker den nye kategori og tryk rediger.
Marker en kategori og tryk slet for at fjerne en kategori, der ikke længere er aktuel.

Features and Functions

- SMS and Email notification (new/changed advisories)
- Generating email lists
- Logging of category changes
- Easy overview of customers due to the grouping concept
- Search on many criteria in the administration system
- Add CVE/CAN number to advisories
- Add Protocol and Port number to advisories
- Report system for statistical information

Questions ???