

CERT.at

**Aufbau eines nationalen CERT
für Österreich**

Begriffe

- CERT

Computer Emergency Response Team

Oft auch:

- CSIRT

Computer Security Incident Response Team



CERT-Aufgaben

■ Incident-Handling

- Triage
 - ◆ Liegt ein Incident vor?
 - ◆ Sind wir zuständig?
 - ◆ Bewerten und Priorisieren.
- Analyse des Vorfalls
- Ergreifen, Vorschlagen, Veranlassen von
- Maßnahmen
- Durchführung und Wirksamkeit kontrollieren
- Nachbereitung



CERT-Aufgaben

- Analog zu „Nebengeschäften“ der Feuerwehr
 - Vermeidung von Vorfällen
 - Mechanismen zur Erkennung
 - Vorbereitung von Gegenmaßnahmen
 - Organisieren von Ansprechpersonen
 - Öffentlichkeitsarbeit
 - Beratung



Was ist ein CERT **nicht**

- Ermittlungsbehörde / Strafverfolgung
- „Silberkugel“ gegen alle Sicherheitsprobleme
- Etwas was man „einschaltet“ und sofort wirksam ist
- Eine Einrichtung die ISOLIERT arbeiten kann
- Eine rein technische Angelegenheit

CERT-Services

Reactive Services



- + Alerts and Warnings
- + Incident Handling
 - Incident analysis
 - Incident response on site
 - Incident response support
 - Incident response coordination
- + Vulnerability Handling
 - Vulnerability analysis
 - Vulnerability response
 - Vulnerability response coordination
- + Artifact Handling
 - Artifact analysis
 - Artifact response
 - Artifact response coordination

Proactive Services



- Announcements
- Technology Watch
- Security Audit or Assessments
- Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

Security Quality Management Services



- ✓ Risk Analysis
- ✓ Business Continuity & Disaster Recovery Planning
- ✓ Security Consulting
- ✓ Awareness Building
- ✓ Education/Training
- ✓ Product Evaluation or Certification

CERTs in Europa



- United Kingdom**
 - BP DSAC
 - BT SBS
 - BTCERTCC
 - Cisco PSIRT
 - CITIGROUP (UK)
 - DAN-CERT
 - E-CERT
 - EUCS-IRT
 - JANET-CERT
 - MLCIRT (UK)
 - MODCERT
 - OxCERT
 - Q-CIRT
 - RBSG-ISIRT
 - RM CSIRT
 - Sky-CERT
 - UNIRAS
- The Netherlands**
 - AAB GCIRT
 - AMC-CERT
 - CERT-IDC
 - CERT-KUN
 - CERT-RUG
 - CERT-UU
 - GOVCERT.NL
 - KPN-CERT
 - SURFnet-CERT
 - UvA-CERT
- Belgium**
 - BELNET CERT
 - NCIRC CC
- France**
 - CERTA
 - Cert-IST
 - CERT-LEXSI
 - CERT-Renater
- Portugal**
 - CERT.PT
- Spain**
 - esCERT-UPC
 - IRIS-CERT

- Germany**
 - CERT-BUND
 - CERTBw
 - CERTCOM
 - CERT-VW
 - ComCERT
 - dCERT
 - DFN-CERT
 - ESACERT
 - FSC-CERT
 - GNS-CERT
 - mCERT
 - Micro-BIT
 - PERMALAN
 - PRE-CERT
 - RUS-CERT
 - S-CERT
 - SAP CERT
 - SECU-CERT
 - Siemens-CERT
 - T-COM-CERT
 - Telekom-CERT
- Ireland**
 - HEANET-CERT

- Iceland**
 - RHnet CERT
- Denmark**
 - CSIRT.DK
 - DK-CERT
 - KMD IAC

- Norway**
 - NorCERT
 - UniNett CERT

- Sweden**
 - SITIC
 - SUNet CERT
 - TS-CERT

- Finland**
 - CERT-FI
 - Ericsson PSIRT
 - FUNET CERT
 - Nokia NIRT

- Estonia**
 - CERT Estonia

- Latvia**
 - LATNET CERT

- Lithuania**
 - CERT-RRT
 - LITNET CERT

- Russia**
 - RU-CERT
 - WebPlus ISP

- Poland**
 - CERT POLSKA
 - PIONIER-CERT
 - TP CERT

- Czech Republic**
 - CESNET-CERTS

- Hungary**
 - CERT-Hungary
 - HUN-CERT
 - NIIF-CSIRT

- Slovenia**
 - SI-CERT

- Croatia**
 - CARNET CERT

- Turkey**
 - TR-CERT
 - Ulak-CSIRT

- Cyprus**
 - CYPRUS

- Luxembourg**
 - CSRRT-LU
- Switzerland**
 - CC-SEC
 - CERN CERT
 - IP+ CERT
 - OS-CIRT
 - SWITCH-CERT
- Italy**
 - CERT-Difesa
 - CERT ENEL
 - CERT-IT
 - CERT-RAFGV
 - GARR-CERT
 - GovCERT.IT
 - S2OC
 - SICEI-CERT

- Malta**
 - mtCERT

- Austria**
 - ACOnet-CERT

- Greece**
 - AUTH-CERT
 - GRNET-CERT

IRT – teams that are using the RIPE IRT object to mark networks they serve

Ausgangslage

- Druck in .at ein CERT zu etablieren ist groß, nicht zuletzt durch internationale Vorbilder
- Auf EU-Ebene werden Projekte forciert
→ Zeitpunkt ist jetzt optimal
- nic.at ist neutraler Nicht-Marktteilnehmer
- Es gibt zahlreiche Rollenvorbilder bei anderen Registries (.ch, .pl, .fi, ...)



Ziele eines nationalen CERTs in .at

- Kontaktpunkt für sicherheitsrelevante IKT-Ereignisse in Österreich
- Vertrauenswürdige, anerkannte Informationsdrehscheibe für diese Themen
- „Der international sichtbare Partner“ für ausländische CERTs
- Koordination von Security-Incidents
- Ressourcenpool für unabhängige Sicherheitsexperten
- Öffentliche Informationen / Awareness



Government-CERT

- In Kooperation mit dem Bundeskanzleramt –
offizielle Ankündigung 21.2.2008 am DP
- Gemeinsame Nutzung der operativen
Ressourcen und internationalen Kontakte
- Constituency: Öffentlicher Sektor
- Zugang zu Informationen anderer Gov-
CERTs



Fallbeispiel

- DDOS / Angriff auf Estland
- Angriff auf das "tägliche Leben" – speziell in einer Gesellschaft mit hohem e-Business Anteil
- Nationales CERT war technische Informationsdrehscheibe für Politik, Presse, Öffentlichkeit und vor allem auch zu internationalen Organisationen

Mehrwert durch Vernetzung

- Lokales CERT übernahm Koordination im Land und Kommunikation zu CERT-FI
- Unterstützung durch FIRST und TF-CSIRT Mitglieder koordiniert durch CERT-FI
 - Entlastung des lokalen Teams
 - Vernetzung mit den weltweit besten Teams
 - Unabhängige "Drittmeinung"
 - → zB Verkehrsanalyse und Bewertung



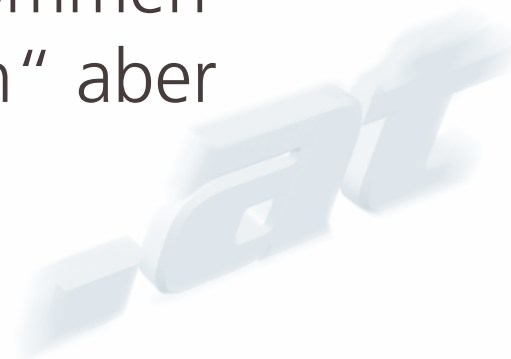
Erfahrungen aus Nachbarländern

- .ch – nach Sektoren getrennte, relativ kleine Expertenrunden (~8-10)
 - + Aufbau einer Vertrauensbasis möglich
 - + Bearbeitung „heikler“ Themen möglich
 - + Wenn Vertrauensbasis da ist, kommt auch entsprechender Input
- Skalierungsprobleme
- Auswahl der Teilnehmer uU schwierig



Erfahrungen aus Nachbarländern

- .de (BSI) – Meldungen werden anonymisiert den Kunden zur Verfügung gestellt
 - + Effizienter Ansatz der gut skaliert
 - Meldungen tw. schwierig zu bekommen – idR möchte gerne jeder „beziehen“ aber keiner „liefern“



Zeitplanung

- Vorbereitungen laufen seit April 2007
- Zahlreiche Gespräche in Österreich
- Aufbau des internationalen Netzwerkes läuft
- **Start „Probetrieb“ 3.3.2008 „nationales CERT“**
- Internationale „Sichtbarkeit“ - Akkreditierungen (TF-CSIRT, FIRST) ~ Mitte März
- Schrittweise Ausdehnung der Services im Laufe des Jahres



Geplante Dienstleistungen

- Incident Handling
 - Meldungen
 - Analyse
 - Response support & coordination
 - Evtl. Bereitstellung von unabhängigen Fachexperten zur Fehlerbehebung / Unterstützung

- Trainings und Awareness Massnahmen
- Alerts & Warnings
 - Öffentliches Informationsservice (frei) – „Endkundentauglich“
 - Spezialisierte Informationskanäle auf Subskriptionsbasis
→ „an Spezialisten gerichtet“

Erste konkrete Aktivitäten

- Mitwirkung an Vorbereitungen zur EURO2008
 - Laufender Austausch mit anderen CERTs
 - Veranstaltung mit Gesundheitsnetz (HEALIX)
 - Landeskrankenanstalten S, OÖ, NÖ & W
 - Einige Landesenergieversorger
 - ÖBB
- Workshops zu Awareness Maßnahmen und Verbesserung der Notfallkommunikation



Ausblick

- Öffentlicher Sektor ist wichtiger Startpunkt
- Einbindung weiterer Projektpartner ist möglich und **erwünscht**
 - zB. ISPA, WKÖ, Energieversorger, Banken, KAV, ...
 - Berater und Hersteller aus Bereich IT-Infrastruktur und IT-Sicherheit
 - Unabhängigkeit muss gewahrt bleiben!
- Weitere Dienste nach Bedarf zB Einbindung in europäisches Sensornetzwerk (ENISA-Projekt)

Kontakt: www.cert.at



TEAM AUSTRIA - COMPUTER EMERGENCY RESPONSE TEAM AUSTRIA - COMPUTER EMERGENCY RESPONSE TEAM AUSTRIA - COMPL

Allgemeines RFC 2350

- **Leitbild**
- Zuständigkeit
- Das Team
- RFC 2350
- Impressum

Leitbild

CERT.at ist das österreichische nationale CERT (Computer Emergency Response Team) das im März 2008 den Probetrieb aufnimmt.

Als solches ist CERT.at der Ansprechpartner für IT Sicherheit im nationalen Umfeld. Es vernetzt andere CERTs und CSIRTs (Computer Security Incident Response Teams) aus den Bereichen kritische Infrastruktur, IKT (Informations- und Kommunikationstechnik) und gibt Warnungen, Alerts und Tipps für KMUs (kleine und mittlere Unternehmen) heraus.

Bei Angriffen auf Rechner auf nationaler Ebene koordiniert CERT.at und informiert die jeweiligen Netzbetreiber und die zuständigen lokalen Security Teams.

Gesammelte Information zu CERT.at sind im [RFC 2350](#) Format abrufbar.

Warum?

Weil IT Sicherheit einen ganzheitlichen Ansatz braucht! Dank unserer immer stärker voranschreitenden Vernetzung gibt es immer mehr Abhängigkeiten zwischen den Systemen. Analog zur Eindämmung von Seuchen gesehen - es braucht eine unabhängige Koordinierungsplattform, die Sicherheitsvorfälle professionell koordinieren kann und andere Netze warnen kann und somit die "Seuchenausbreitung" eindämmen kann.

Nur durch die Koordination der Einzelbestrebungen kann in Summe mehr IT Sicherheit erreicht werden.