Das neue NIS-Gesetz und aktuelle Cyber-Bedrohungen …

… und der richtige Umgang mit Vorfällen

Mag. Robert Schischka, CERT-Direktion,
nic.at-Geschäftsführung

Wer sind wir?

GovCERT AUSTRIA

CERT.at

- **CERT.at – das nationale Computer Emergency Response Team**
  - Ansprechpartner für IT Sicherheit im nationalen Umfeld
  - Zielgruppe: österreichische IT Security-Teams und lokale CERTs
  - Vernetzung von und mit anderen CERTs, Sicherheitsteams (weltweit)
  - Koordinationsstelle
  - Initiative von nic.at (österreichische Domain Registry)

- **GovCERT – das Government Computer Emergency Response Team**
  - Zielgruppe: öffentliche Verwaltung und kritische Informationsinfrastruktur
  - Kooperation zwischen Bundeskanzleramt und CERT.at

Informationen

Warnungen

Schwerwiegende Sicherheitslücke in Microsoft Office - aktiv ausgenützt

25. März 2014

Beschreibung

Microsoft hat ein Security Advisory zu einer schwerwiegenden Sicherheitslücke (CVE-2014-1761) in einer Komponente von Microsoft Office veröffentlicht. Die Schwachstelle wird laut Microsoft bereits in gezielten Attacken aktiv ausgenützt.

Die Schwachstelle kann dazu benutzt werden, auf den PCs von Benutzern, die ein präpariertes RTF-File öffnen oder betrachten, beliebigen Code mit den Rechten des angemeldeten Benutzers auszuführen.
Es ist zu erwarten, dass entsprechende Dateien bald via zum Beispiel Spam-Mails verteilt oder auf entsprechenden Webseiten zum Download angeboten werden.

Es besteht auch der Verdacht, dass momentan an Adressen in Österreich versandte Spam-Mails mit Subjects wie "A1 Rechnung 5795377 von 24-03-14" und einem gefälschten Absender der A1 Telekom, genau diese Lücke auszunutzen versuchen.

Auswirkungen

Da der Angreifer prinzipiell beliebigen Code auf betroffenen Systemen ausführen kann, sind alle Daten auf diesen Systemen, sowie potenziell alle durch diese erreichbaren (etwa durch ausspionierte Zugangsdaten, VPN, Fileshares, etc.) Daten und anderen Systeme gefährdet.

Betroffene Systeme

Systeme, auf denen folgende Versionen von Microsoft Office installiert sind, sind betroffen:

- Microsoft Word 2003 Service Pack 3
- Microsoft Word 2007 Service Pack 3
- Microsoft Word 2010 Service Pack 1 (32-bit editions)
- Microsoft [illegible] Service Pack [illegible]

Tageszusammenfassung

[CERT-daily] Tageszusammenfassung - Freitag 11-04-2014

Daily end-of-shift report team at cert.at
Fri Apr 11 18:25:29 CEST 2014

- Previous message: [CERT-daily] Tageszusammenfassung - Donnerstag 10-04-2014
- Next message: [CERT-daily] Tageszusammenfassung - Montag 14-04-2014
- **Messages sorted by:** [date] [thread] [subject] [author]

```
=======================
= End-of-Shift report =
=======================

Timeframe:    Donnerstag 10-04-2014 18:00 - Freitag 11-04-2014 18:00
Handler:      Alexander Riepl
Co-Handler:   Stephan Richter


*** Heartbleed vendor informations / statistics ***
------------------------------------------------
```

https://isc.sans.edu/diary/Heartbleed+vendor+notifications/17929
https://www.cert.fi/en/reports/2014/vulnerability788210.html
http://securityaffairs.co/wordpress/23878/intelligence/statistics-impact-heartbleed.html

```
*** Gehackte Online-Konten: Mehr als zehn Millionen Abrufe von
Sicherheitstest ***
------------------------------------------------
Auch der zweite Sicherheitscheck des BSI zu gehackten Online-Konten
stößt auf großes Interesse. Für Verwirrung sorgt aber weiter eine
Sicherheitssperre von GMX und web.de.
------------------------------------------------
```

http://www.golem.de/news/gehackte-online-konten-mehr-als-zehn-millionen-abrufe-von-sicherheitstest-1404-105787-rss.html

NIS-RICHTLINIE

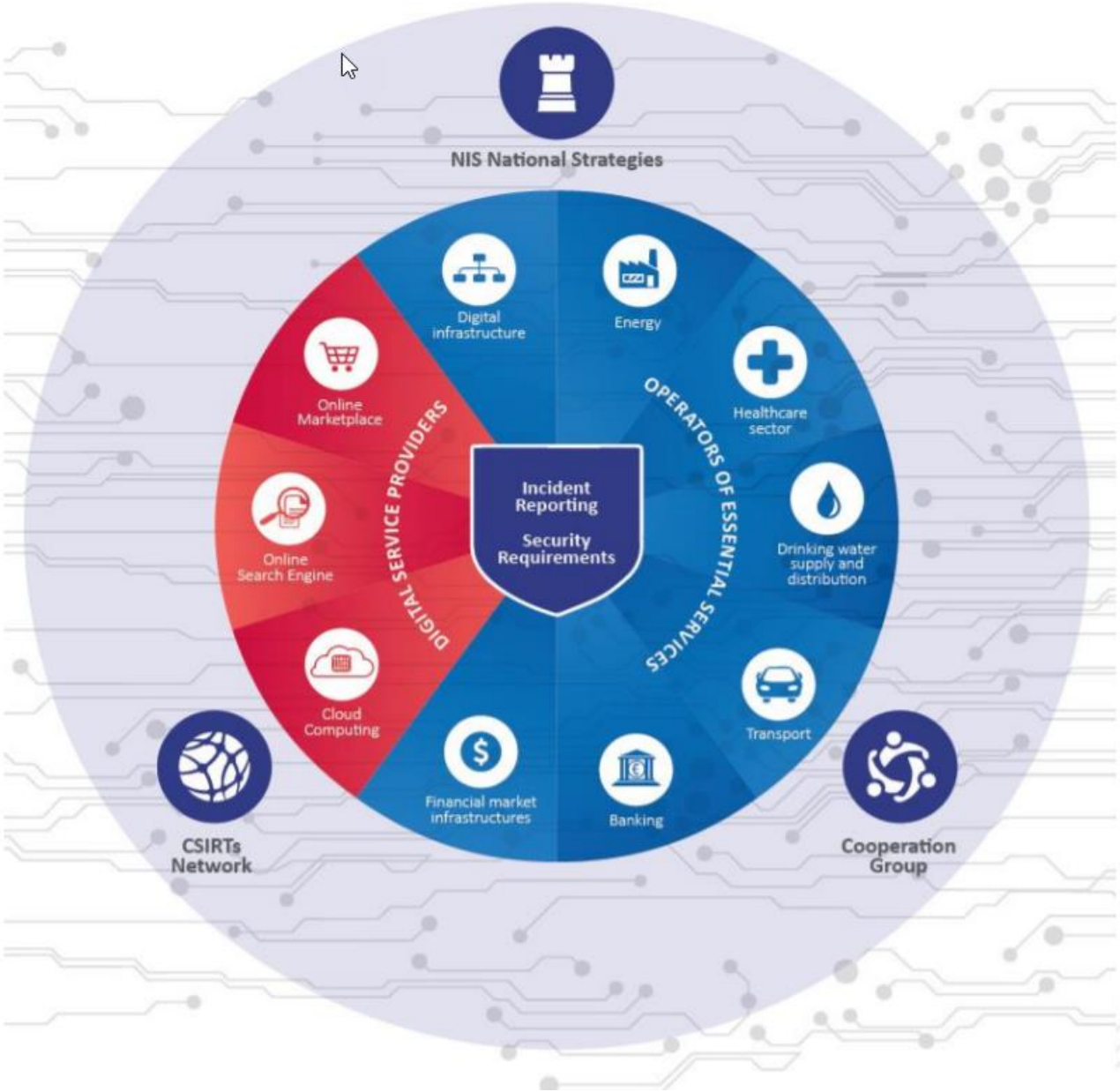
RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union

GRUNDSÄTZLICHES ZUR RICHTLINIE

- **Ziele**
  - Erreichung eines hohen gemeinsames Sicherheitsniveau von Netzen und Informationssystemen in der Union
  - Verbesserung des Funktionierens des Binnenmarktes
- **“Minimum-Harmonisierung”**
  - MS dürfen - abweichend von den Regelungen in der Richtlinie - Bestimmungen erlassen, die ein höheres Sicherheitsniveau von Netzen und Informationssystemen ermöglichen
    (siehe auch „Überlegungen zur Umsetzung in Österreich“)
  - Bestimmte Bereiche sind von dieser Regelung aber explizit ausgenommen

WESENTLICHE INHALTE DER RICHTLINIE

- Verpflichtung zur Festlegung einer nationalen NIS-Strategie
- **Ermittlung betroffener Unternehmen**
- **Verpflichtungen für betroffene Unternehmen**
  - Mindest-Sicherheitsanforderungen
  - Meldepflichten
- Einrichtung nationaler Behörden und Organisationen
- Einrichtung von Gremien zur internationalen Zusammenarbeit
- **Aufsichtsfunktion der NIS-Behörden**


NIS National Strategies
Digital infrastructure
Energy
Healthcare sector
Drinking water supply and distribution
Transport
Banking
Financial market infrastructures
Cloud Computing
Online Search Engine
Online Marketplace
DIGITAL SERVICE PROVIDERS
OPERATORS OF ESSENTIAL SERVICES
Incident Reporting
Security Requirements
CSIRTs Network
Cooperation Group

KRITERIEN ZUR ERMITTLUNG

- **Ermittlung von “Betreibern wesentlicher Dienste”**
  - Bereitstellung eines Dienstes, der für die Aufrechterhaltung kritischer gesellschaftlicher und/oder wirtschaftlicher Tätigkeiten unerlässlich ist
  - Bereitstellung ist von Netzen und Informationssystemen abhängig
  - Sicherheitsvorfall würde erhebliche Störung der Bereitstellung bewirken
- **“Erhebliche Störung”**
  - Definition muss bestimmte **sektorübergreifende Faktoren** berücksichtigen, u.a. Marktanteile des Unternehmens, sektorübergreifende Abhängigkeiten, Substituierbarkeit des Dienstes, betroffene Nutzer und geografische Ausdehnung

BETREIBER WESENTLICHER DIENSTE

- Geeignete und verhältnismäßige **technische und organisatorische Maßnahmen** (“Stand der Technik”), um Risiken zu bewältigen
- Maßnahmen, um Auswirkungen von Sicherheitsvorfällen vorzubeugen bzw. diese so gering wie möglich zu halten
- **Meldeplicht für Sicherheitsvorfälle** „die erhebliche Auswirkungen auf die Kontinuität der […] wesentlichen Dienste haben“ an die zuständige Behörde (oder CSIRT)
- Unternehmen unterliegen einer **“ex-ante”-Aufsicht** durch die zuständige Behörde

ANBIETER DIGITALER DIENSTE

- Geeignete und verhältnismäßige **technische und organisatorische Maßnahmen** (“Stand der Technik”) in bestimmten Bereichen, um Risiken zu bewältigen
- Maßnahmen, um Auswirkungen von Sicherheitsvorfällen vorzubeugen bzw. diese so gering wie möglich zu halten
- **Meldeplicht für Sicherheitsvorfälle** „die erhebliche Auswirkungen auf die Bereitstellung [des] Dienstes haben“ an die zuständige Behörde (oder CSIRT)
- Unternehmen unterliegen einer **“ex-post”-Aufsicht** durch zuständige Behörde (bei Nachweis für Pflichtverletzungen)

AUFSICHTSFUNKTION DER BEHÖRDEN

"Betreiber wesentlicher Dienste"	"Anbieter digitaler Dienste"
▪ "**ex-ante**"-Aufsicht	▪ "**ex-post**"-Aufsicht (bei Vorliegen von Nachweisen für Pflichtverletzungen)
▪ Informationsbereitstellungspflicht zur Bewertung des Sicherheitsniveaus	▪ Informationsbereitstellungspflicht zur Bewertung des Sicherheitsniveaus
▪ Nachweis der wirksamen Umsetzung der Sicherheitsmaßnahmen durch **Audits** (durch Behörde oder extern)	
▪ Zuständige Behörde darf **verbindliche Anordnungen** erteilen	▪ NIS-Behörde darf **Abstellung der Pflichtverletzung** anordnen

Umsetzungspflichten für Unternehmen

- **Sicherheitsvorkehrungen**
  - geeignet, um hohes Sicherheitsniveau von NIS zu gewährleisten
  - dem Stand der Technik entsprechend
  - technisch und organisatorisch
  - Nachweis
- **Meldepflichten**
  - unverzügliche Meldung eines Sicherheitsvorfalls beim zuständigen Computer-Notfallteam (CSIRT)
  - Mitwirkungspflicht
  - freiwillige Meldungen

Sicherheitsvorkehrungen

- Treffen von **geeigneten organisatorischen und technischen Vorkehrungen** in Hinblick auf betriebene wesentliche Dienste
- Stand der Technik
- BKA kann durch VO **Mindestsicherheitsmaßnahmen** festlegen
- Vorschlag von sektorenspezifischen Sicherheitsvorkehrungen von Betreibern wesentlicher Dienste möglich
- Grundsätzlich wird versucht „nichts neues zu erfinden“
- Bezugnahme auf anerkannte, verbreitete Standards

Qualifizierte Stellen zur Überprüfung

- Überprüfung der BwD durch qualifizierte Stellen oder durch das BMLV (wenn es der Aufgabenerfüllung des Bundesheeres dient)
  - Regelmäßiger Nachweis der Überprüfungen gegenüber BMI
  - BwD haben mindestens alle drei Jahre die Erfüllung der Anforderungen dem BMI nachzuweisen
- Qualifizierte Stelle = „NIS-Prüfungsstelle“
  - spezielle Erfordernisse werden durch VO des BMI festgelegt
  - Antragstellung an BMI / ex lege
  - BMI kann qualifizierte Stellen überprüfen

Meldepflicht - Inhalt

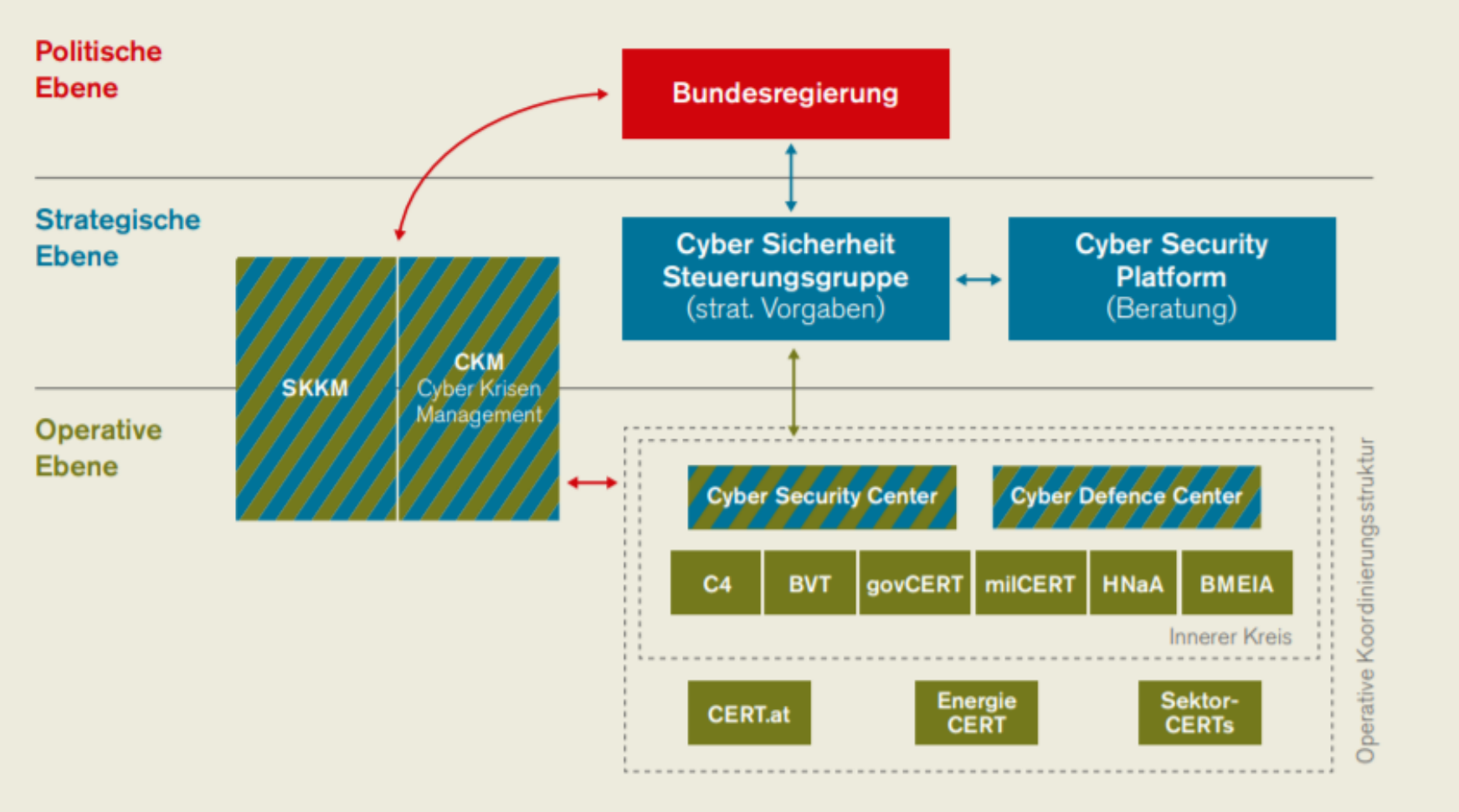
- Angaben
  - zum Sicherheitsvorfall
  - zu technischen Rahmenbedingungen, insb.
    - vermutete oder tatsächliche Ursache
    - betroffene Informationstechnik,
    - Art der betroffenen Einrichtung oder Anlage
- Alles was im **Zeitpunkt der Meldung** bekannt ist
- Angaben über später bekanntgewordene Umstände sind nachzureichen
- Geläufiges elektronisches Format unter Verwendung festgelegter Kommunikationskanäle (**Meldeformular**)

Meldepflicht

- Meldung von Sicherheitsvorfällen an zuständiges **Computer-Notfallteam (CSIRT)**
- Erstmeldung **unverzüglich**
- Nachmeldungen ohne unangemessene weitere Verzögerung
- CSIRT leitet unverzüglich an BMI weiter

- **Freiwillige Meldungen**
  - Betreiber eines nicht wesentlichen Dienstes oder Störungen, die kein Sicherheitsvorfall sind
  - werden ebenfalls an BMI weitergeleitet
    - aggregierte Weitergabe der Meldungen
    - Nennung kann auf Verlangen entfallen

Cyber Sicherheit in Österreich



WO WIR NICHT HINWOLLEN:

„Der Pathologe weiß alles ganz genau …
aber leider zu spät“

MELDERECHTE

- Staatliche Meldepflichten sind **kein Ersatz für freiwillige Kooperation**
- **Freiwilliger Informationsaustausch** MUSS zwischen den (potenziell) Betroffenen möglich sein
  - zeitnah und umfassend
  - auch abseits von Meldepflichten – z.B. Schwellwerten
  - auf Wunsch anonymisiert
  - auf einer gesicherten rechtlichen Basis
  - Ohne, dass sofort Ermittlungsverfahren gegen den Willen der Betroffenen eingeleitet werden

ROLLE DER CSIRTs/CERTs

- Daher soll eine **Vernetzung und ein Informationsaustausch innerhalb der Branchen** gefördert werden
- Die ÖSCS sieht die Möglichkeit der **Selbstorganisation** durch eine Branche vor → siehe Energy-CERT
- Branchen-CERTs liefern Input in den Lagebildprozess
- Damit sollen zwei **Ziele** erreicht werden
  - Unternehmen sind selbst besser informiert und können rascher reagieren
  - Verdichtete Informationen tragen zu einem bessern Lagebild bei

Aktuelle Trends

- DDOS Angriffe: Spitzenwerte bis 1,7 Tbs (!)
- Mobile Malware
- POS-Malware
- Prozessor-Schwachstellen werden uns begleiten
- Ransomware, Cryptominer etc.
- Spass mit IoT

- Verstärkt Angriffe auf Unternehmen
  - CEO Fraud
  - Erpressungen bei Datenverlust
  - Social Engineering

Aktuelle Trends

- Datendiebstahl
  - PII – personally identifiable information
    - Gesundheitsdaten, Sozialversicherung, Bankdaten …
- Organisierte Banden
  - spezialisierte Software
  - Aufwendige Vorbereitung der Infrastruktur
    - Money Mules, Call Center, Dropzones, Phishing Sites …
    - Infrastruktur zum Abtesten gestohlener Credentials
  - Arbeitsteiliges Vorgehen ist auch hier best practice
- CaaS: Crimeware as a Service

Grundregel

Cybercrime ist nicht durch die verfügbaren Infektionen limitiert, sondern durch die Fähigkeit, diese zu Geld zu machen.

Die schlechte Nachricht

- Irgendwann „erwischt“ es jeden einmal
  - Technische Komplexität nimmt eher zu als ab, egal was die Hersteller versprechen
  - Kostendruck und Forderungen an Umsetzungsgeschwindigkeit helfen auch eher den Angreifern
  - Faktor „Mensch“ ist eine zentrale Schwachstelle

→ Zumindest sollte man davon ausgehen verwundbar zu sein

Schadensminimierung

- Wie schnell wurde ein Vorfall erkannt?
  - Normalzustand vs. Anomalie (z.B. in Netzen)
  - Melden sich Betroffene→ Awareness & Kultur
- Wie rasch kann reagiert werden?
  - Definierte Teams CERTs? Bereitschaft? 7x24?
- Wie konsequent und umfassend wird reagiert?
  - Reserven? Technisch / personell
  - Ausdehnungspotenzial bewerten
  - Ursache bekämpfen oder „Melanom überschminken“
  - Welche Befugnisse haben Incident Handler / Betrieb?

?

Mag. Robert Schischka
schisch@cert.at

www.cert.at
Cert-Hotline: 01/505 64 16 78