CERT.at – Das nationale CERT

Wos is mei Leistung?

Dimitri Robl
<robl@cert.at>

2019-05-02

Programm

- CERT/CSIRT – Was ist das?
- Rahmenbedingungen in Österreich
  - Einbettung
  - NIS Gesetz
- Kooperation und Datenaustausch
- Services und Tooling

whoami

Name: Dimitri Robl

Position: Incident Handler bei CERT.at seit 2018-10-01

Mini-CV:

- Was mit Sprachen an der Uni Wien studiert
- Dann Systemadministrator ebenfalls an der Uni Wien

CERT vs. CSIRT

CERT™

- “Computer Emergency Response Team”
- Trademarked by cert.org (CMU)

CSIRT

- “Computer Security Incident Response Team”
- Keine Trademark

→ Keine inhaltlichen Unterschiede

CERT/CSIRT Aufgaben

- IT Sicherheitsteam
- Klar definierte Aufgabe
- Von außen sicht- und ansprechbar
- Leistungen festgelegt in RFC 2350
- Hat nichts mit Zertifikaten, X.509, ISO27k, etc. zu tun ;)

Arten von CERTs/CSIRTs

- In “normalen” Firmen
  - IT Sicherheitsverantwortlicher/-team
  - PSIRT (Product Security Incident Response Team)
- In ISPs
  - abuse-Handling
  - Network und Server-Security
- Übergreifend
  - Sektorenspezifisch (Energie, Finanz, etc.)
  - Government CERT
  - Nationales CERT
  - Länderübergreifend, z.B. ENISA

CERT.at im Detail

Nationales CERT für Österreich

- Teil der nic.at in Kooperation mit dem Bundeskanzleramt → Public-Private-Partnership
- *Nicht* Teil einer Behörde

Aufgaben

Proaktiv: Warnungen, Pressearbeit, Community-Building, Networking,...

Netzwerkhygiene: Betroffene über Probleme ihrer Netzwerke/Homepages/Server/etc. informieren

Reakiv: Hilfe bei Vorfällen

Rahmenbedingungen

- Keine Weisungsrechte
- Meldepflicht nur für Betreiber wesentlicher Dienste gemäß NIS Gesetz
- Zuständig für das ganze Land

Was geht trotzdem?
→Überraschend viel!

Staatliche Strukturen

Rechtlicher Rahmen

- Österreichs Strategie für Cyber-Sicherheit
- NIS-Richtlinie (EU) 2016/1148: Grundlage zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der EU.
- NIS Gesetz

NIS Directive in a Nutshell

- Identifikation wesentlicher Dienstleistungen
  - Mindeststandards für IT-Sicherheit
  - Meldepflicht bei Vorfällen
- National Etablierung von
  - CSIRTs/CERTs
  - zuständigen Behörden
- Kooperation in der EU
  - CSIRTs-Network
  - Kooperationsgruppe

Umsetzung in AT

- Gesetz trat 2018-12-28 in Kraft
- Zuständige Behörden:

  Strategisch: Bundeskanzleramt (BKA)

  Operativ: Cyber Security Center (CSC)
- Aufgaben und Anforderungen an CERTs
  - Meldestellen für Pflicht- und freiwillige Meldungen
  - Unterstützung im Notfall
  - Für alle, nicht nur Betreiber wesentlicher Dienste

Operative Ebene

- Operative Koordination
  - CERT.at, Sektor-CERTs/CSIRTs
  - IKDOK (Innerer Kreis Der Operativen Koordinationsstruktur):

BKA	Abteilung I/8: Cyber Security, GovCERT, NIS Büro und ZAS
BMI	CSC im BVT, C4 im Bundeskriminalamt
BMLV	MilCERT, HNaA, AbwA
BMEIA	

  - Krisenmanagement in das Staatliche Krisen- und Katastrophenschutzmanagement (SKKM) integriert
  - EU: CSIRTs Network

Strategische Ebene

- Cyber Security Steuerungsgruppe (CSS)
  - Oberstes Koordinationsgremium auf Beamtenebene
  - Zuarbeitende Gruppen eine Ebene darunter
- Cyber Security Platform (CSP): Forum Wirtschaft/Verwaltung
- Cooperation Group

Datenschutz

- Aufgaben der CSIRTs erstmals klar definiert → Rechtssicherheit
- Meldepflicht/-recht
  - Rechtssicherheit für Betroffene
  - Responsible Disclosure nicht explizit enthalten
- Datenaustausch zwischen den Behörden

Kooperationen National

- CERT.at/GovCERT/Austrian Energy CERT (AEC)
- IKDOK
- Operative Koordinationsstruktur (OpKoord)
- CERT-Verbund
- Austrian Trust Circle (ATC): Sektoren der kritischen Infrastruktur
- ArgeSecur
- Kuratorium Sicheres Österreich (KSÖ)

Kooperationen International

- Forum of Incident Response and Security Teams (FIRST): Globaler Dachverband
- TF-CSIRT: Europäischer Dachverband
- CSIRTs Network
- European GovCERT Group (EGC)
- Central European Cyber Security Platform (CECSP)
- CERT-Verbund Deutschland
- Diverse Trust-Groups

</Abstraktionen>

- Genug Theorie, was bedeutet das alles konkret?
- Wie schaut das Tagesgeschäft aus?
- Welche
  - Tools?
  - Daten?

Hard-Core Technik?

- Arbeit des nationalen CERTs ist nur $< 5\%$ tief Security-technisch
- Sondern
  - Informationsdrehscheibe
  - Vernetzung von Personen/Institutionen
  - Vermittlung
  - Pressearbeit
  - Awarenessbuilding

Aufgaben von CERT.at Revisited

Proaktiv: Warnungen, Pressearbeit, Community-Building, Networking,...

Netzwerkhygiene: Betroffene über Probleme ihrer Netzwerke/Homepages/Server/etc. informieren

Reakiv: Hilfe bei Vorfällen

Tech-Watch

Wir müssen wissen, was los ist und veröffentlichen relevante Infos:

- Warnungen wenn
  - Vorfall eine große Reichweite hat
  - Autoupdates nicht greifen
  - Es Gegenmaßnahmen gibt → kein “Fürchtet euch!”

  Zugang:
  - Webseite
  - Mailingliste
- Tageszusammenfassungen: Täglicher Überblick zu aktuellen Updates, Vorfällen, Entwicklungen, etc.
  - Mailingliste
  - Archiv zum Nachlesen

Tool: Taranis (github-Repo) vom NCSC.nl

Networking

- Konferenzen
- Regelmäßige Treffen
  - monatlicher IT Security Stammtisch gemeinsam mit der Uni Wien
  - CERT-Verbund
  - Austrian Trust Circle (ATC)
- Mailinglisten: s.o.

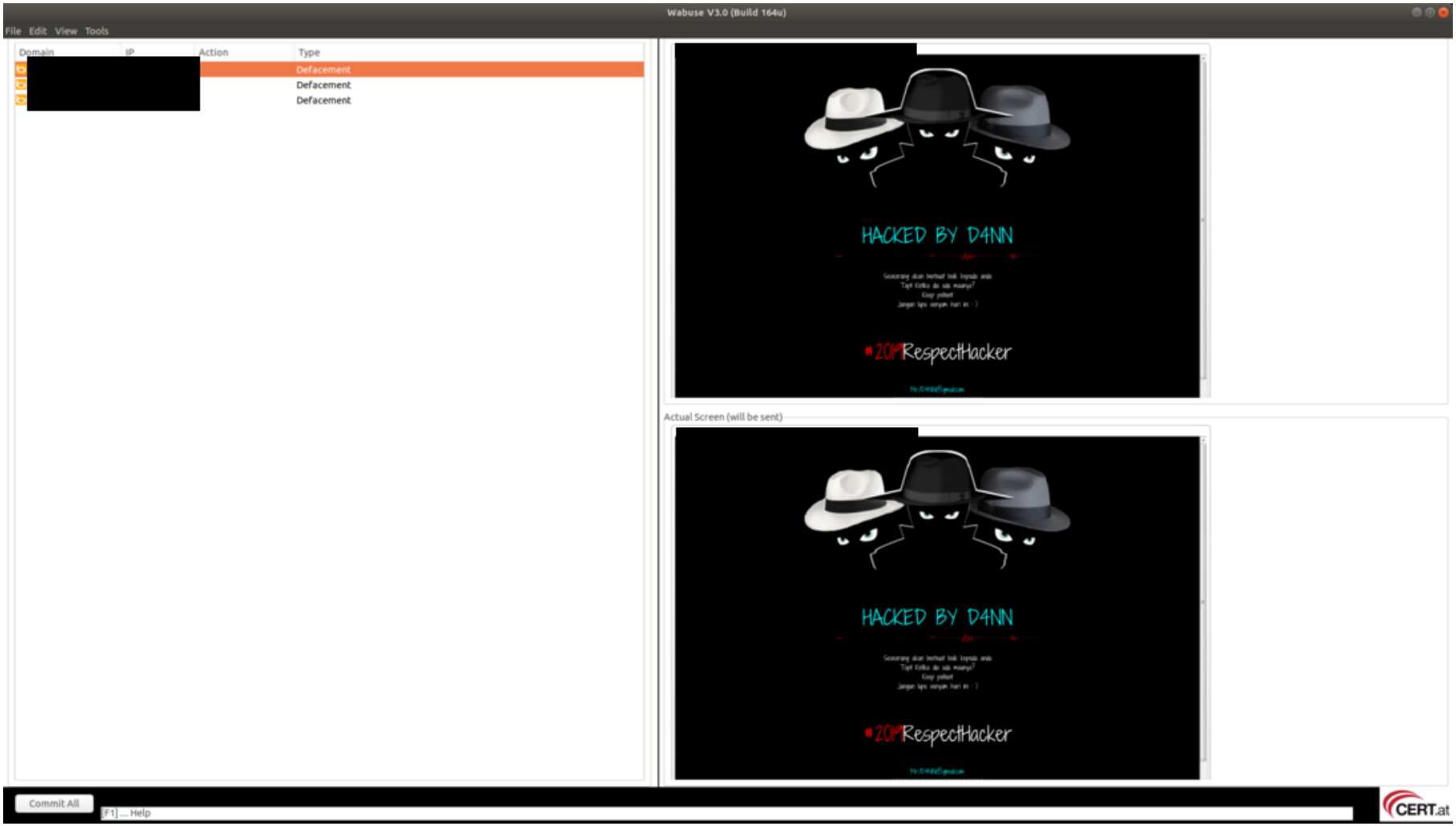
Netzwerkhygiene

- Web
  - Defacements
  - Phishing
  - Exploit-Packs
  - SEO Spam Injection
- Infektionen
  - Botnetze
  - Kommunikation mit C&C-Server (Sinkholes)
- Vulnerable Devices
  - Fehlkonfigurationen
  - Veraltete Protokolle (SSLv2, CharGen, etc.)
  - DDoS Reflektoren

Datenquellen

- CERT/CSIRT + IT-Security Community
- Non-Profit Organisationen:
  - Shadowserver
  - Spamhaus
  - ...
  - Unabhängige Researcher*innen
- For-Profit Organisation
  - Google/Bing Malicious URLs feeds
  - Microsoft Digital Crimes Unit
  - shodan.io
  - Zone-H
- Eigene Recherchen

Beispiel Webhacks



Ablauf Webhacks

Eingehend	• Listen von URLs • Manchmal auch Metadaten
Bearbeitung	• Händisch mit Wabuse (s.o.)
Ausgehend	• Mails an zuständige Personen (Registrare, Hosting Plattform, etc.)

Ablauf Infektionen und Vulnerable Devices

Eingehend
- Meist `.csv`-Files
- Enthalten IP-Adressen und Metadaten

Bearbeitung
- Automatisiert mit IntelMQ (s.u.)
- *Keine* manuelle Prüfung der Daten

Ausgehend
- Mail an ISPs (abuse-Kontakte)
- Liste aller gemeldeten Probleme im jeweiligen Netzwerk

IntelMQ

- Open Source Tool zur automatisierten Verarbeitung von Feeds
- IntelMQ Github Repo
- Github Repo zum graphischen Interface
- Ablauf:
  - Sammelt und parsed Feeds die wir erhalten
  - Verarbeitet, dedupliziert und reichert die Daten an
  - Schickt die Ergebnisse weiter
- Arbeitet automatisiert mit unserem Ticket-System, damit alles dokumentiert ist

IntelMQ – About

- Python
- Verwendet Message Queueing Protokoll
- Messages in JSON
- Mailinglisten:
  - https://lists.cert.at/cgi-bin/mailman/listinfo/intelmq-users
  - https://lists.cert.at/cgi-bin/mailman/listinfo/intelmq-dev
- Leicht erweiterbar
- Wird von einigen CERTs/CSIRTs produktiv eingesetzt

“Oneshots”

- Neue Lücke für die es (noch) keine Feeds gibt
- Auffindbar über shodan.io/Daten maschinenlesbar vorhanden? Wenn ja:
  1. Passende Query basteln bzw. passenden Parser finden
  2. Daten in ein `.csv`-File konvertieren
  3. Template-Text für die Aussendung schreiben
  4. Alles zusammen in IntelMQ einkippen
  5. Betroffene werden automagisch informiert
- Hilfreich wenn
  - Zeit kritisch ist
  - neue Feeds getestet werden sollen
  - regelmäßige Aussendungen nicht sinnvoll sind

Threat Intel

- Wie geht eine bestimmte Malware/eine bestimmte Gruppe vor?
- Indicators of Compromise (IoCs), z.B.
  - Hashes
  - IPs
  - Filenamen
  - URLs
  - ...
- Alleine kaum bewältigbar → Sharing is caring!
- Aber wie? Email? o.O

MISP – Malware Information Sharing Platform

- Webseite
- Github Repo
- Open Source Community Projekt
- Informationen in maschinenlesbarer Form abgreifbar
- Synchronisation zwischen Instanzen möglich
- Das Tool der Wahl für CERTs/CSIRTs
- CERT.at betreibt eine Instanz auf der Firmen/Behörden Accounts erhalten können
- Bei Interesse: team@cert.at

Responsible Disclosure

- Bieten wir für Probleme mit Österreichbezug an
- Reaktionen auf Schwachstellenreports sehr unterschiedlich
- Von Bug-Bounties bis zu (juristischen) Drohungen → Was tun?
- Bei Unsicherheit: CERT.at als Relay verwenden; Kontakt: reports@cert.at
- Anonymität gegenüber der betroffenen Entität
- Direkter Kontakt kann auf Wunsch jederzeit hergestellt werden

Abschließend

- Feedback zu unserer Arbeit ist sehr willkommen!
- Wer unsere Infos bekommen will, muss funktionale Abuse-Kontakte haben ;)
- Updates, Updates, Updates

Fragen?