CyberHilfsWerk - Konzeption für eine Cyberwehr 2.0

Johannes ‚ijon' Rundfeldt

Wer ist die AG KRITIS?

- ca. 35 aktive Mitglieder
- Alle dienstlich im KRITIS-Umfeld unterwegs
- Kennen gelernt und Gründung im Dunstkreis des Chaos Computer Club
- Seit August 2019 unabhängig vom CCC e.V.

zu meiner Person

- Johannes “Ijon” Rundfeldt
- 2011 Erstkontakt mit KRITIS im Rahmen der Arbeit für Jimmy Schulz MdB, damals Mitglied der EIDG (Enquete Komission Internet und digitale Gesellschaft)
- Mitarbeiter von Jimmy Schulz MdB in der 17. WP und 19.WP
- Themen: IT-Security, Netz- und Digitalpolitik, KRITIS

Jetzt Alarm schlagen!

- Bisher keine Großschadenslage, nur kleinere Störungen
- Aber: Eintrittswahrscheinlichkeit einer Großlage steigt
- Großflächiger Ausfall nur noch eine Frage der Zeit!
- IT-Sicherheit verbessern reicht nicht mehr. Wir brauchen richtige Krisenbewältigungskapazitäten

Eintrittswahrscheinlichkeit einer Großlage steigt.

- Digitalisierung und Vernetzung beschleunigt sich
- Anlagen werden früher unsicher, vor Ende der geplanten Lebensdauer
- Großflächige Ausfälle der IT durch Malware werden häufiger (Emotet, notpetya…)
- Hackback-Bestrebungen gefährden Infrastruktur

Kapazitäten des Staates

- Diverse Kapazitäten die nur für die staatliche Verwaltung bereit stehen
  - CERT-Bund, Verwaltungs-CERT-Verbund
- CERT-Verbund
  - Staatliche Kapazitäten und CERTs von großen Unternehmen. → "Information-Sharing"
- BSI MIRT (Mobile Incident Response Team)
  - Ca 10-30 Personen, tatsächliche Incident Response

weitere Informationen auf Bundestags Drucksache 19/2645

Katastrophenübungen

- LÜKEX
  - LÜKEX11 hatte Bezug zu digitalen Angriffen
  - Nur "Stabsrahmenübung"
  - LÜKEX21, Thema: "„Cyberangriff auf Regierungshandeln"
- Locked Shields
  - Zwar Übung von Angriffen auf technische Anlagen
  - Aber ohne Bewältigung der Krisensituation aus Sicht der Betreiber von KRITIS

Katastrophenübungen

- Kleinere, lokale Übungen
  - z.B. “Umschalten auf Netzersatzanlage” in Krankenhäusern
- Keine Übungen von Großschadenslagen
- Keine Übungen von technisch orientierten Szenarien auf Seiten der Betreiber → “Tschernobyl-Trauma”
- Keine Szenarien, die so groß sind, das die vorhandenen Kapazitäten diese nicht bewältigen können

Katastrophenübungen

- Keine Übungen, die den flächigen Ausfall von IT-Monokulturen simulieren. (Windows, Microsoft Office, Citrix, Oracle, SAP etc)
- “Informationstechnologie” ist nicht nur “KRITISV Anhang 5” sondern inzwischen die **technische Betriebsgrundlage aller Sektoren**

Übungsziele

- Große Übungen, Ziel jeweils: “Staats- und Regierungsbetrieb sicherstellen”
- Keine Übungen die sich mit der **Wiederherstellung der Versorgung der Bevölkerung** beschäftigen

Zusammenfassung Problem

- Zuwenig Incident Response Kapazitäten
- Keine ausreichenden Übungen
- Sehr wenig staatliche Kapazitäten für Incident Response (IR)
- Großflächige Ausfälle von Infrastruktur werden kommen
- Verbesserung der IT-Sicherheit und Betriebssicherheit reicht nicht, es braucht mehr staatliche IR-Kapazität

Wer stellt die Versorgung der Bevölkerung wieder her?

Wer ergänzt, wenn das MIRT und das CERT-Bund ausgelastet sind?

Was fehlt?

- Ehrenamtliche / zivile Kapazitäten
- Erfolgsmodelle (für andere Szenarien):
  - Freiwillige Feuerwehr
  - Technisches Hilfswerk (THW)
  - Deutsches Rotes Kreuz (DRK)

Wir brauchen ein CHW!

- Arbeitstitel
- „**C**yber**H**ilfs**W**erk“
- Metapher:
  - MIRT = Berufsfeuerwehr
  - CHW = freiwillige Feuerwehr

Unser Ziel:

Das CHW soll die existierenden Bewältigungskapazitäten für Großschadenslagen durch Cybervorfälle bei Kritischen Infrastrukturen kooperativ ergänzen.

Die Idee ist nicht neu, oder?

- „Da bräuchte ich mal von Ihnen eine Krisennummer.“ (Bundesminister des Inneren Thomas de Maiziere, 2015 zum Vorstand des CCC e.V.)
- CCC e.V. leider ungeignet
- CCC-Mitglieder erkennen aber den Bedarf!

2014 – BSI-Versuch “Cyberwehr”

- Leider gescheitert
  - (illegale) Arbeitnehmerüberlassung
  - Schwierigste Kartellrechtliche Fragen
  - (Software)-Lizenzrechtliche Fragen
  - Unklare Vergütung / Entschädigung

Aufgaben eines CHW

- Unterstützung hauptamtlicher Kräfte
- Bündelung und Ausbildung ziviler Helfer
- Digitaler Katastrophenschutz
- Schutz der Bevölkerung vor Auswirkungen von Ausfällen
- Behebung von Einschränkungen in der Versorgung mit kritischen Dienstleistungen

Szenario “Malware”

- WannaCry, Emotet, Notpetya
- Wiederherstellung der Systeme ist personalintensiv
- Neuvergabe von Passwörtern ist personalintensiv

Szenario “Krankenhaus”

- Sicherheitslücken in HL7-Protokoll möglich / wahrscheinlich
- HL7 ist weit verbreitet und lässt sich kaum kurzfristig austauschen oder upgraden
- Sicherheitslücken ermöglichen überregionalen Angriff auf Systeme
- Bei erfolgreichem Angriff würden die staatlichen Kapazitäten nicht reichen um alle Krankenhäuser gleichzeitig wieder online zu bringen

Szenario “Wasserversorgung”

- Kaum Incident Response Fähigkeiten im Bereich “Wasser”
- IT und OT kann Anlagen dazu bringen bakteriell “unrein” zu werden
- (Fast) alle Anlagenbetreiber gehen davon aus, das im Krisenfall die Anlagen von Hand gefahren werden können
- Bei massivem, großflächigem Cyberangriff kann dies aber nicht mehr garantiert werden

Szenario “Monokulturen”

- Große Software-Monokulturen entstehen um uns herum
- Citrix, Microsoft, Oracle, Telematik-Infrastruktur … usw
- Neue Sicherheitslücken benötigen in Monokulturen unglaublich schnelle Reaktion und Updates
- Überregionale Monokulturen vervielfachen notwendigen Personaleinsatz zur Behebung der Krise

Szenario “IoT Waschmaschine”

- Hypothetisches Szenario
- 1Mio Waschmaschinen * 3kW Heizelement = 3GW
- Zukünftig alle am Internet - mit NTP auch präzise synchronisiert
- 3GW Schaltleistung, synchronisiert zur Netzfrequenz – keine technische Möglichkeit die Netzfrequenz auszugleichen
- Europaweite Stromausfälle drohen
- **Vor Wiederanfahren des Stromnetz** müssen alle Geräte aktualisiert oder entnetzt werden.

Alarmierung des CHW

- Nicht durch Unternehmen oder Privatpersonen
- Ausschliesslich bei “Großlagen” (Staat entscheidet über Großlagen! - siehe THW – Alarmierung nur durch BMI)
- MIRT ist “Berufsfeuerwehr” - rücken zuerst aus.
- CHW wäre dann “freiwillige Feuerwehr” - kann nachgefordert werden
- Juristisch sauberster Weg den Helfern offizielle Handlungskompetenzen zu geben - “Verwaltungshelfer”

Ausbildung

- Vereinheitlichung und Standardisierung ist für Vertrauen von Behörden und Betreibern wichtig!
- Themen
  - Ethische Grundsätze (Datenschutz, Hackerethik, responsible Disclosure)
  - Kommunikation und Team-Management
  - Krisenkommunikation
  - Grundlagen IT, OT, ICS, SCADA, Prozessleitsysteme
  - Einschätzen von Situationen zum Selbstschutz

Ausbildungszentren

- Privatpersonen haben kaum Zugang zu OT-Hardware
- Ausbildungszentren bauen! (“fachspezifische Spielwiesen”)
  - Große Leitstände
  - Komplexe ICS-Systeme
  - Prozessleittechnik und Gebäudeleittechnik
  - Spezielle Branchensoftware (Lizenzen)
- THW und Feuerwehr haben sowas auch
  - Brückenbau, Atemschutz

Vertrauensproblem in der Community

- Problembewusstsein ist weit verbreitet in der Community
- Behörden werden meist eher kritisch gesehen oder gemieden
  - BSI hat eher gutes Image
  - BMI hat eher kein gutes Image
- Schutz vor offensiven Einsätzen ist notwendig

Kooperation ja, aber: “on our Terms”

- „on our Terms“ → Vertrauen & Engagement der Community!
- Kein Durchgriff von Sicherheitsbehörden auf CHW
- Werkzeuge (Dual Use) die die Community für CHW ehrenamtlich entwickelt oder spendet, müssen beim CHW bleiben
    - Keine Weitergabe an Sicherheitsbehörden
- Die Rechtsform des CHW muss hier Schutzfunktion erfüllen

Rechtsform des CHW

- Noch keine finale Präferenz
- aber eine Analyse verschiedener Ideen
- Entscheidung muss mit Behörden zusammen gefällt werden

Rechtsform des CHW
Modell: DRK

- Gemeinnütziger eingetragener Verein
- Freiwillige Kooperationsvereinbarung mit Staat
- (-) Vorhaltungen für Katastrophenschutz ist ideeler Bereich – rein Spendenfinanziert
- (+) unabhängig vom BMI

Rechtsform des CHW
Modell: Fachgruppe des THW

- THW ist eine Bundesanstalt
- (-) Grundausbildung verpflichtend notwendig (ca 150h)
- (+) Bereits in der Fläche etabliert
- (+) starker ziviler Fokus – offensive Einsätze sind ausgeschlossen

Rechtsform des CHW
Modell: SEE des THW

- THW ist eine Bundesanstalt
- (-) Grundausbildung verpflichtend notwendig (ca 150h)
- (-) Sondereinsatzeinheiten (SEE) haben zentrale Natur
- (+) starker ziviler Fokus – offensive Einsätze sind ausgeschlossen

Rechtsform des CHW
Modell: Angliederung an MIRT / BSI

- (-) BSI steht unter Fach- und Rechtsaufsicht des BMI
- (-) vollständiger Ausschluss offensicher Einsätze juristisch eher schwierig
- (+) kurze Dienstwege, beste Kommunikation

Rechtsform des CHW
Modell: eigene Bundesanstalt CHW

- (-) größerer behördlicher und politischer Aufwand
- (-) größerer Abstand zum THW – Symbiosen schwieriger
- (+) ermöglicht eigene Gesetzgebung (CHW-Gesetz) – damit auch die größte Flexibilität
- (+) beste Garantie auf rein defensiven Einsatz

Haftung

- Keine (Haftungs-) Belastung der ehrenamtlichen Helfer
- Haftung nur bei grober Fahrlässigkeit oder Vorsatz
- Eigene Regelung denkbar (CHW-Gesetz)
- “Spontanhelfer” bzw “Verwaltungshelfer”-Status würde auch reichen

Versicherung

- Je nach Katastrophe und Organisation
  - Ländersache oder
  - Bundessache (Unfalkasse Bund)
- Automatisch, wenn man “Verwaltungshelfer” ist.

Freistellung und Kostenerstattung

- Ähnlich wie bei THW
- Wenn der Einsatz vom BMI ausgerufen wird, dann müssen die Arbeitgeber die THW-Helfer unter ihren Mitarbeitern freistellen
- Entschädigung in Höhe des Bruttolohns vom Staat an Arbeitgeber
- Auch für Selbstständige - “THW Entschädigungsrichtlinie”

Konzept v1.0 “CHW”

- PDF ab **jetzt verfügbar** auf https://ag.kritis.info
- Gerne weitergeben!
- Konzept wird weiterentwickelt – Input höchst erwünscht!

Vielen Dank!

- Fragen? Dann jetzt!
- Danke für die Aufmerksamkeit
  - Twitter: @AG_KRITIS
  - Website: http://ag.kritis.info
  - Twitter privat: @ijonberlin