Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Wirtschaft, Bildung und Forschung WBF

Bundesamt für Wirtschaftliche Landesversorgung BWL
Fachbereich IKT

Cyberrisiken in Spitälern

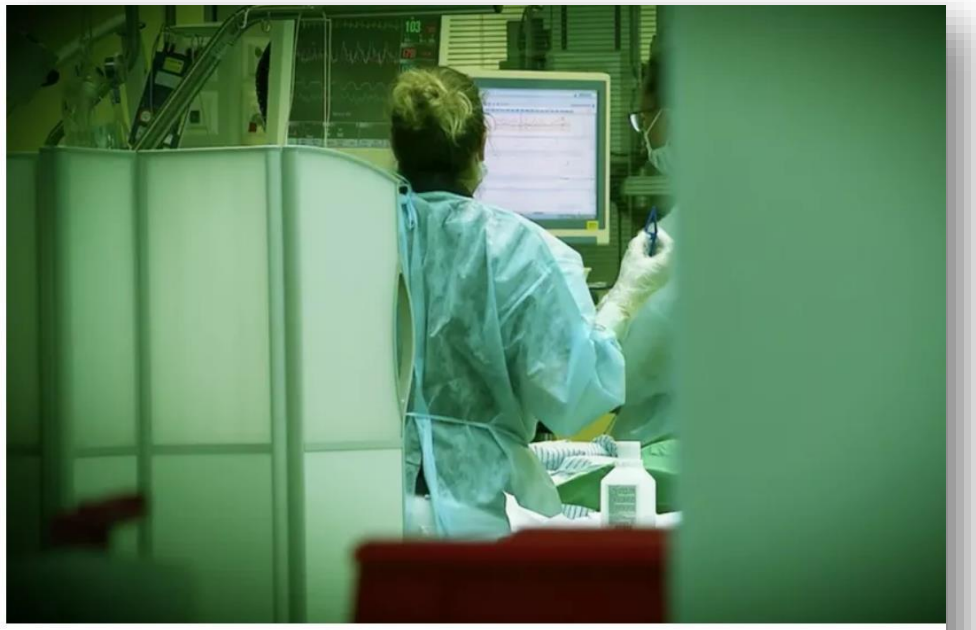
Aktuelle Lage und empfohlene Massnahmen

Daniel Caduff
Bundesamt für wirtschaftliche Landesversorgung BWL
Stv. Leiter Geschäftsstelle IKT

Spitäler: Besondere Herausforderungen

- Anders als bei anderen Kritischen Infrastrukturen sind Spitäler offen zugänglich
- Es gibt Systeme wie z.B. Herz-Lungen-Maschinen, bei denen Cyberangriffe potenziell tödlich sind
- Ein Spital hat teilweise hunderte verschiedene Geräte von verschiedenen Herstellern im Einsatz → Wartung und Übersicht sind extrem schwierig
- Zertifizierung von medizinischen Geräten verbietet die nachträgliche Änderung der Software → keine Updates möglich
- In Spitälern werden kritische Systeme von Ärzten und Pflegepersonal bedient → keine Cyberprofis

Spitäler: Cyberangriff Spital Wetzikon



Krankenhäuser geraten zunehmend ins Visier von Cyberkriminellen.

«Gefährlichste Malware der Welt» attackiert Zürcher Spital – das musst du wissen

Fachleute bezeichnen Emotet als derzeit gefährlichste Schadsoftware der Welt. Kürzlich hat es ein Spital im Kanton Zürich erwischt. Hier sind die wichtigsten Fragen und Antworten rund um den Cyberangriff.

- Das Spital Wetzikon wurde 2019 Opfer eines Ransomwareangriffs (EMOTET als Dropper)
- Es mussten verschiedene medizinische Geräte temporär ausser Betrieb genommen werden.
- Der Angriff wurde schnell erkannt und konnte wirksam eingedämmt werden.
- Aber:
  - Ärzte hatten keinen Zugriff auf Patientenakten.
  - Operationen mussten verschoben werden
  - Untersuchungen konnten nicht. durchgeführt werden.

Beispiel: Cyberangriff Hirslanden-Gruppe

Neue Zürcher Zeitung

Cyberangriff auf die Hirslanden-Gruppe: Die Spitäler sind wegen der Pandemie besonders anfällig für Erpressungen

Die Pandemie macht Gesundheitseinrichtungen zu einem lohnenden Ziel von Cyberkriminellen. Entsprechend bietet der Bund Unterstützung an – doch nicht alle nehmen sie an. Die Hirslanden-Gruppe wurde Opfer eines Angriffs.

Lukas Mäder

25.11.2020, 05.30 Uhr

- Im Juli 2020 wurde die Hirslanden-Gruppe mit der Schadsoftware «Trickbot» angegriffen.
- Publik wurde der Fall erst Ende 2020.
- Gemäss der Hirslanden-Gruppe hatten die Angreifer sich bin die zentralen Netzwerkkomponenten / Server vorgearbeitet.
- Daten seien keine gestohlen worden.
- Ebenfalls seien keine Patientendaten verschlüsselt worden, sondern nur administrative Unterlagen.
- Alle Dateien konnten dank Backups wiederhergestellt werden.
- Die Beeinträchtigung dauerte 6 Tage.

Beispiel: Cyberangriff Pallas Kliniken

Grosser Cyber-Angriff auf Schweizer Privatklinikgruppe

Klinik , Pallas Kliniken , Cyberattacken , Hirslanden , It , It-sicherheit

Veröffentlicht am: 14. August 2021 13:01 , von cm | Letzte Aktualisierung: 16. August 2021 15:04

Verständnis und bitten Sie um Entschuldigung. Wir sind aktuell nur telefonisch erreichbar unter Tel: +41 58 335 00 00. Wir danken für Ihr Verständnis und bitten Sie um Entschuldigung. Wir sind aktuell nur te

Pallas Kliniken

Augen Haut / Venen Schönheit Team Zuweiser/Externe Standorte Über uns

Die Pallas Kliniken sind Opfer eines Hacker-Angriffs geworden. | Screenshot Webseite Pallas Kliniken

Hacker haben die Pallas Kliniken angegriffen und die Informatik-Systeme lahmgelegt. Patientendaten seien aber nicht betroffen, versichert das auf Augenheilkunde und ästhetische Medizin spezialisierte Spital.

«Wir sind aktuell nur telefonisch erreichbar. Wir danken für Ihr Verständnis und bitten um Entschuldigung.» Dies steht noch immer **auf der Webseite der Privatklinikgruppe Pallas**, die in der Schweiz 20 Standorte betreibt. Seit Donnerstag sind die Informatik-Systeme «down», wie zuerst der «Tages-Anzeiger» berichtet.

- Im August 2021 war die private Klinikgruppe «Pallas Kliniken» von einem Ransomeware-Angriff betroffen.
- Mehrere IT-Systeme waren daraufhin nicht mehr verfügbar. Um eine weitere Ausbreitung zu verhindern, wurden die Systeme darauf kontrolliert heruntergefahren.
- Mehrere geplante Behandlungen konnten nicht durchgeführt werden und Patienten mussten zum Teil wieder nach Hause geschickt werden.

Safety vs. Security

- Safety = Sicherheit von Menschenleben
- Security = Informationssicherheit
- Safety kommt immer vor Security

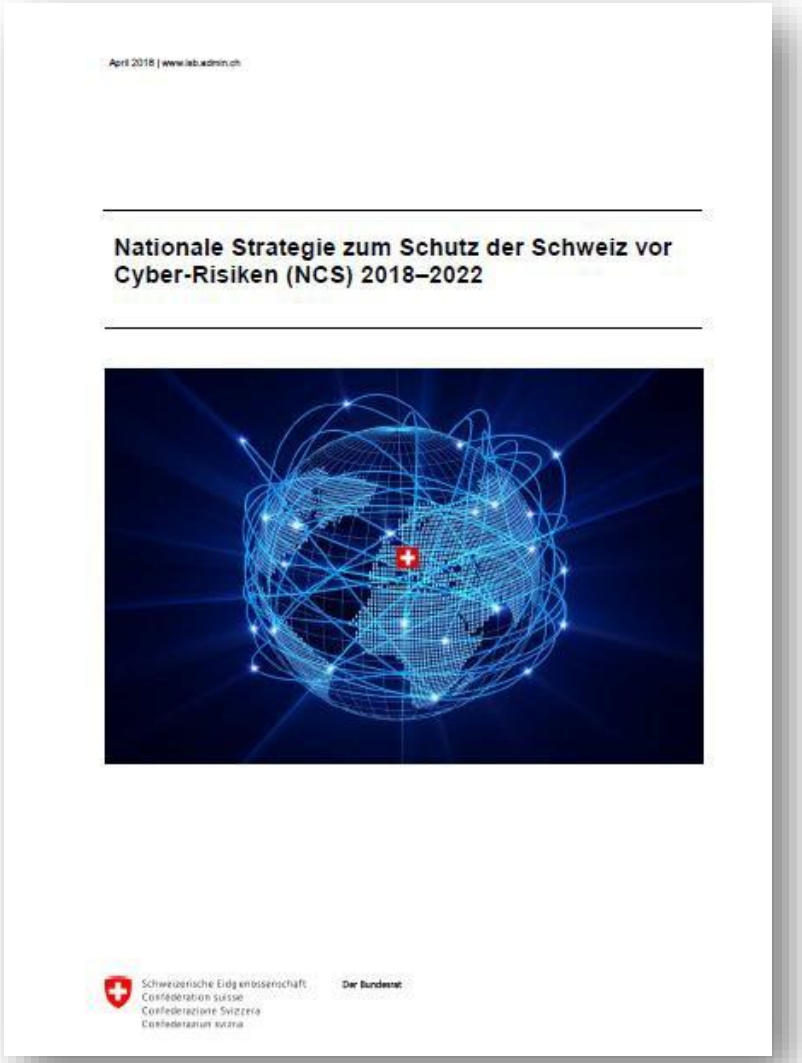
- Cyberrisiken können beides sein: Safety- und Securityrelevant

- Datenschutzverletzungen sind Security-Relevant, jedoch nicht Safety-Relevant

- Angriffe auf Cyber-physische Syteme (z.B. MRI, Beatmungsmaschine, Dialyse-Gerät) sind potenziell tödlich für Patientinnen und somit Safety-Relevant!

- Verfügbarkeit kommt vor Datenschutz!

Strategie zum Schutz der Schweiz vor Cyberrisiken NCS



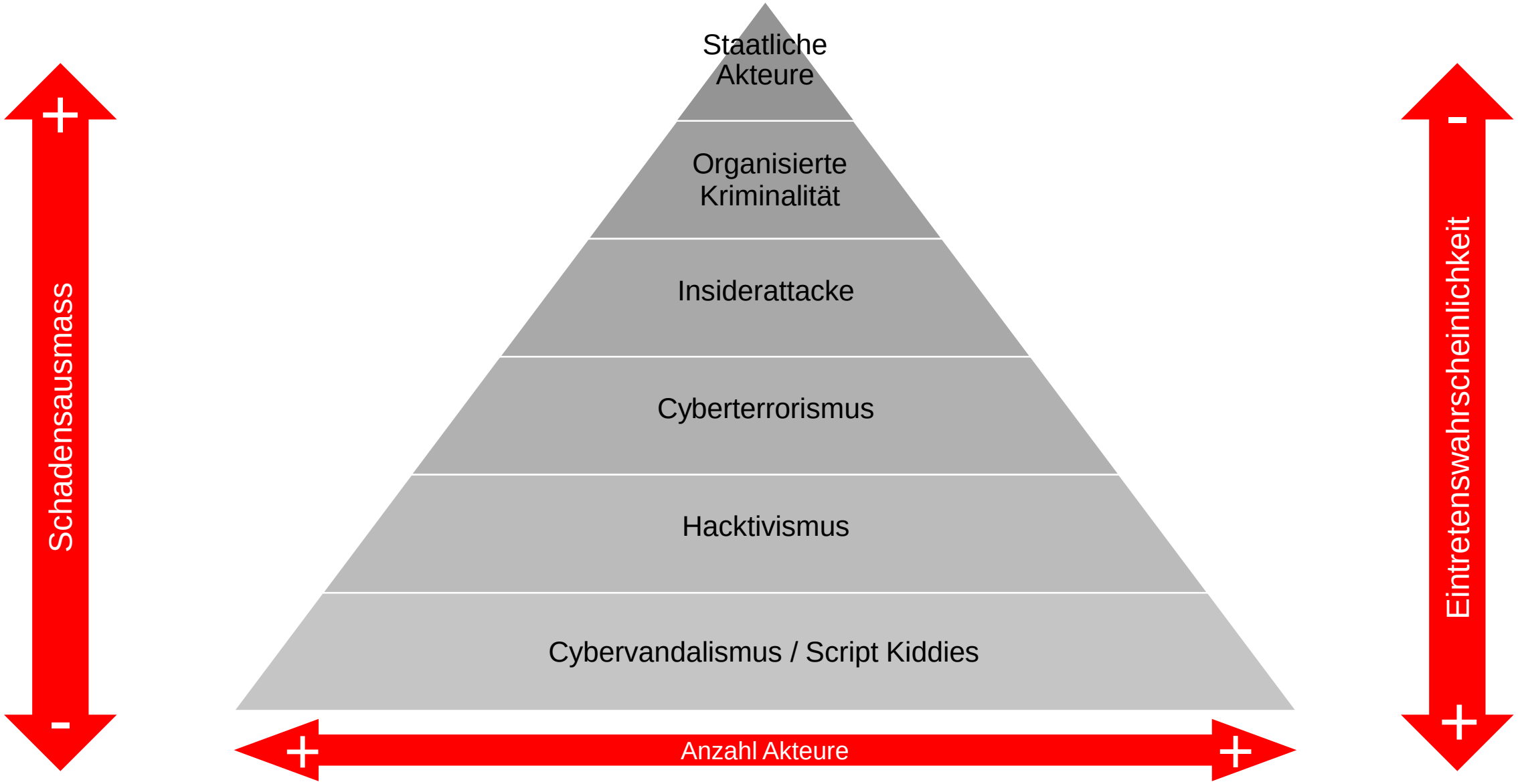
- Der Bundesrat hat 2012 die «Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken» beschlossen (NCS).
- Das BWL hat zusammen mit verschiedenen Branchenverbänden IKT-Minimalstandards entwickelt
- Der vorliegende (generelle) Minimalstandard ist eine präventive Massnahme zur Stärkung der IKT-Resilienz im Sinne der NCS.
- Der spezifische Standard für Spitäler befindet sich aktuell in Arbeit.

Aufgabenteilung Cyber im Bund

Aufgaben:

- Verteidigung (Cyberdefence)
- Strafverfolgung (Cybercrime)
- Schutz kritischer Infrastrukturen (Cybersecurity)
- Organisatorische Trennung, aber enge Zusammenarbeit und gegenseitige Absprache.

Risikopyramide



IKT Minimalstandard

- Der Standard ist universell einsetzbar
- Der primäre Fokus liegt auf kritischen Infrastrukturen
- Der Standard gibt vor, *was* zu tun ist, lässt dem Anwender aber die Freiheit zu entscheiden, *wie* er es tun möchte
- Der Standard ist kompatibel mit internationalen Industriestandards, wie z.B. ISO-Standards

Downloadlink der Standards und Hilfsmittel

Ziele des Standards

- Cybersicherheit, umfasst die Vertraulichkeit, Integrität und Verfügbarkeit von Daten.
- Mit dem IKT-Minimalstandard stellt die WL Unternehmen ein vielseitig einsetzbares Hilfsmittel zur Verfügung.

Vertraulichkeit

- Patientendaten
- Personaldaten
- Buchhaltung
- …

→ z.T. gesetzliche Vorschriften, jedoch nicht safety-relevant.

Integrität

- Z.B. Patientendaten
- Labordaten / Messwerte

→ Falsche Messwerte / Labordaten können zu Behandlungs-fehlern führen
→ **Safety-relevant!**

Verfügbarkeit

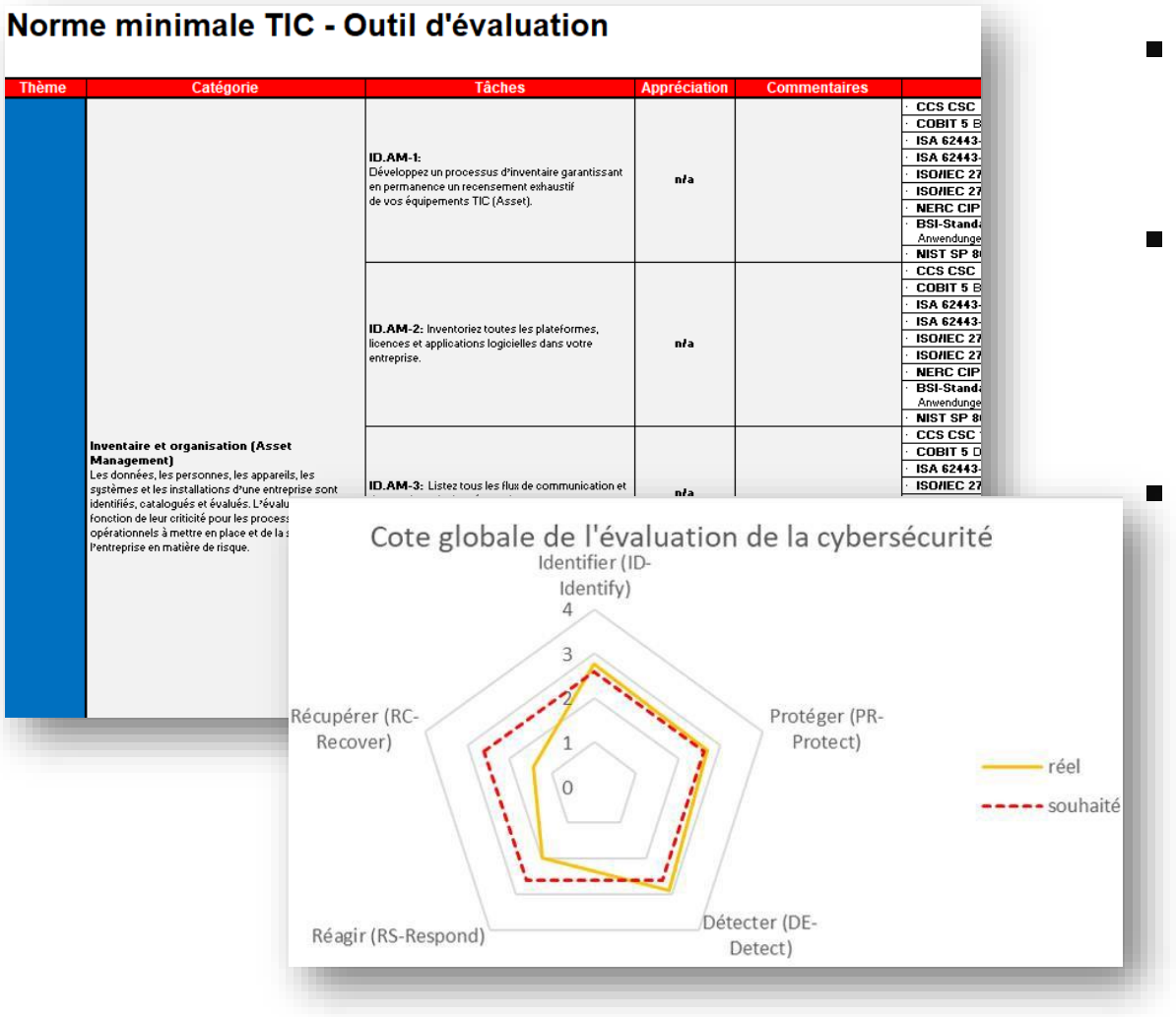
- Patienteninforma-tionssystem
- Cyber-physische Systeme

→ Manipulation / Ausfall einer Herz-Lungen-Maschine ist potenziell tödlich.
→ **Safety-relevant!**

Wie funktioniert der Standard?

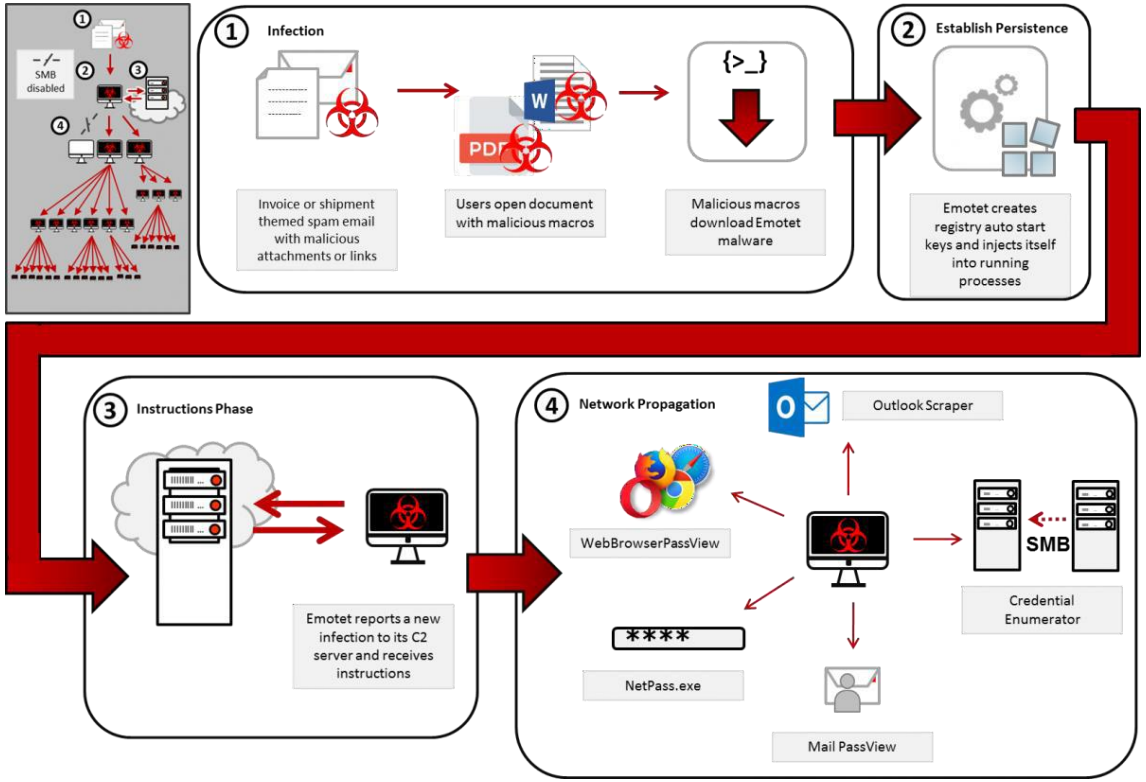
- Der Standard wurde von den Experten der wirtschaftlichen Landesversorgung entwickelt und gliedert sich in 5 Kapitel.
- Zu jedem Kapitel empfiehlt der Standard spezifische Aktivitäten.
- Insgesamt sind es 106 Aktivitäten, deren Umsetzung zwischen 0 bis 4 bewertet wird.

Wie funktioniert der Standard?



- Zur Umsetzung stellt der Bund ein Excel-Tool zur Verfügung.
- Die Bewertung der 106 Aktivitäten erlaubt dem Anwender eine Beurteilung seines Schutzniveaus.
- Der Standard ist risikobasiert und auditierbar.

Aktuelle Bedrohungslage: Ransomware EMOTET / Trickbot / Ryuk



- EMOTET ist ein Trojaner, der oft via E-Mail verbreitet wird (Anhang oder gefälschter Link)
- Anschliessend verbreitet sich EMOTET selbständig weiter, indem er z.B. alle E-Mail Adressen kopiert, die er finden kann.
- EMOTET funktioniert als «Dropper» und kann je nach Bedarf ein unterschiedliches Arsenal an «Werkzeugen» mitführen. Aktuell z.B. oft die Ransomware «Ryuk» oder den E-Banking-Trojaner «Trickbot».
- EMOTET hat auch erfolgreich Schweizer Firmen attackiert: Meier Tobler, Offix, Lobsinger Marazzi und das Spital Wetzikon!
- Internationale Opfer: U.a. Kammergericht Berlin, und mehrere US-Stadtverwaltungen! (Pensacola, New Orleans, u.a.)

Aktuelle Bedrohungslage: Ransomware «WannaCry»

- Verbreitet sich selbständig als Wurm
- Nützt längst bekannte Schwachstelle in Windows XP aus
- Verantwortlich für den Ausfall von mehreren kritischen Infrastrukturen insb. Spitälern in UK
- Viele Privatpersonen und Firmen verlieren Daten
- Geschätzter Umsatz: ca 50 Millionen USD

Erfolgreiche Ransomware Angriffe in der Schweiz

Cyberangriff kostet Meier Tobler Millionen

Weil Hacker die gesamte IT-Infrastruktur der Haustechnikerfirma Meier Tobler lahmlegten, konnte das Unternehmen während vier Arbeitstagen keine Waren ausliefern. Nun ist klar: Der Schaden geht in die Millionenhöhe.

Das Unternehmen Meier Tobler ist Händler und Serviceanbieter für Gebäudetechnik
(Quelle: Meier Tobler AG)

Informatik lahmgelegt

Schweizer Firmen von Hacker-Angriff betroffen

Gestern, 12:01 Uhr
Aktualisiert um 22:46 Uhr

Dieser Artikel wurde **48**-mal geteilt.

- Seit Donnerstag sind die Informatiksysteme der französischen Baufirma Bouygues Construction durch einen Cyberangriff lahmgelegt.
- Wie Recherchen von SRF zeigen, sind davon auch Schweizer Unternehmen betroffen.
- Es handelt sich dabei um die beiden Tochterunternehmen Losinger Marazzi AG mit Sitz in Bern und das Gebäudetechnik-Unternehmen Bouygues Energies & Services (früher Alpiq Intec) mit Sitz in Zürich. Bei Bouygues sind nur die Mails betroffen.

- Nur eine Auswahl von erfolgreichen Angriffen («Spitze des Eisberges»)
- Alle Arten von Unternehmen können betroffen sein
- Auch Kritische Infrastrukturen betroffen (u.a. Spital Wetzikon)

Offix von massivem Hacker-Angriff getroffen

SECURITY, ECOMEDIA, HACKERANGRIFF,

Von Katharina Jochum, 03. Juli 2019 16:14 Letzte Aktualisierung: 31. Dezember 2019 15:30

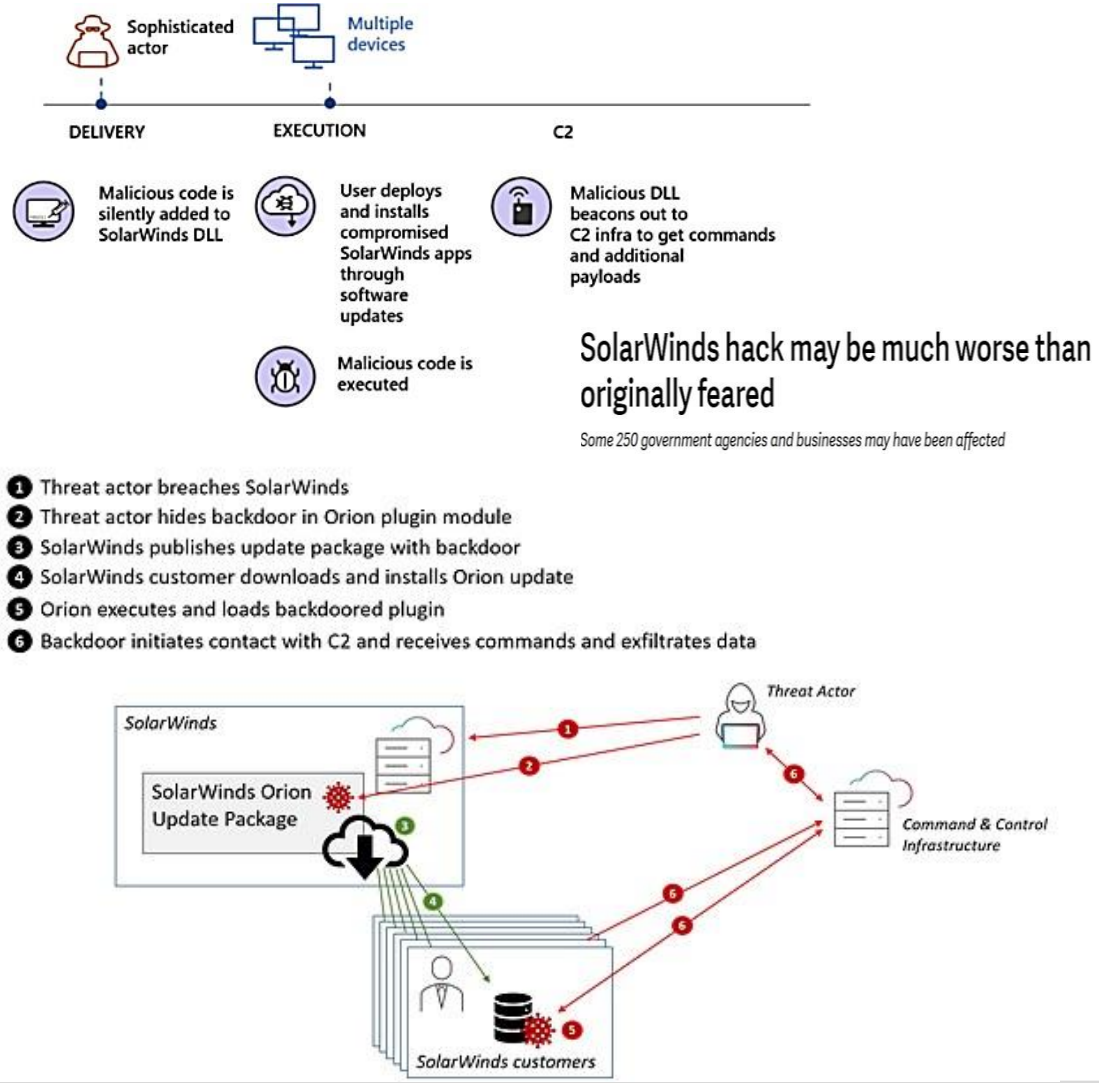
Das Ransomware-Trio Emotet, Trickbot und Ryuk hat die IT-Systeme der Offix-Gruppe lahmgelegt. CEO Martin Kelterborn erklärt den Ablauf des Hackerangriffs im Gespräch mit inside-it.ch

Das Ransomware-Trio Emotet, Trickbot und Ryuk hat die IT-Systeme der Offix-Gruppe lahmgelegt. CEO Martin Kelterborn erklärt den Ablauf des Hackerangriffs im Gespräch mit inside-it.ch.

«Wir hatten ein Riesenglück» – das Spital Wetzikon wurde vom derzeit aggressivsten Trojaner angegriffen

Viele Schweizer Spitäler unterschätzen das Risiko von Cyberangriffen. Verpflichtende Mindeststandards für die interne IT-Sicherheit gibt es nicht. Doch das könnte sich ändern.

Aktuelle Bedrohungslage: Supply-Chain-Angriff Solar Wind hack auf Fire Eye



- SolarWinds ist ein grosses IT-Unternehmen, das Software für Einrichtungen von Fortune-500-Unternehmen bis hin zur US-Regierung anbietet.
- Der Angriff blieb monatelang unentdeckt und hätte Daten in den höchsten Ebenen der Regierung, einschliesslich des US-Militärs und des Weissen Hauses, offenlegen können.
- Durch ein Update welches Malware enthielt wurden bis zu 18’000 Organisation zum Opfer.
- Das Update sollte eigentlich eine Sicherheitslücke schliessen.
- Schadensausmass von bis 100 Milliarden US Dollar.

Aktuelle Bedrohungslage: DDOS

de fr it

Zürich 18°

Schweiz Ausland Wirtschaft Sport People Entertainment Digital Wisse

News E-Spo

Ihre Story, Ihre Informationen, Ihr Hinweis? feedback@20minuten.ch

Miese Masche

22. Mai 2013 14:40; *Akt: 22.05.2013 15:49*

Schweizer Web-Shops werden erpresst

von Daniel Schurter - Unbekannte bedrohen die Betreiber von populären Verkaufsplattformen mit einer DDoS-Attacke. Wer nicht bezahlt, muss mit teuren Folgen rechnen. Ein Betroffener wehrt sich.

- Simpel, aber effektiv
- Server werden so lange mit konzentrierten Anfragen überhäuft, bis diese dem Ansturm nicht mehr stand halten können.
- Lässt sich heute auch als illegale Dienstleistung mieten («Hacking as a Service»)

Aktuelle Bedrohungslage: Phishing

Bund warnt vor gefälschten «Swiss»-E-Mails mit Retefe im Anhang

Achtung vor diesem E-Banking-Trojaner: Kriminelle versenden gefälschte E-Mails in Namen der Fluggesellschaft Swiss.

swiss.com

SWISS

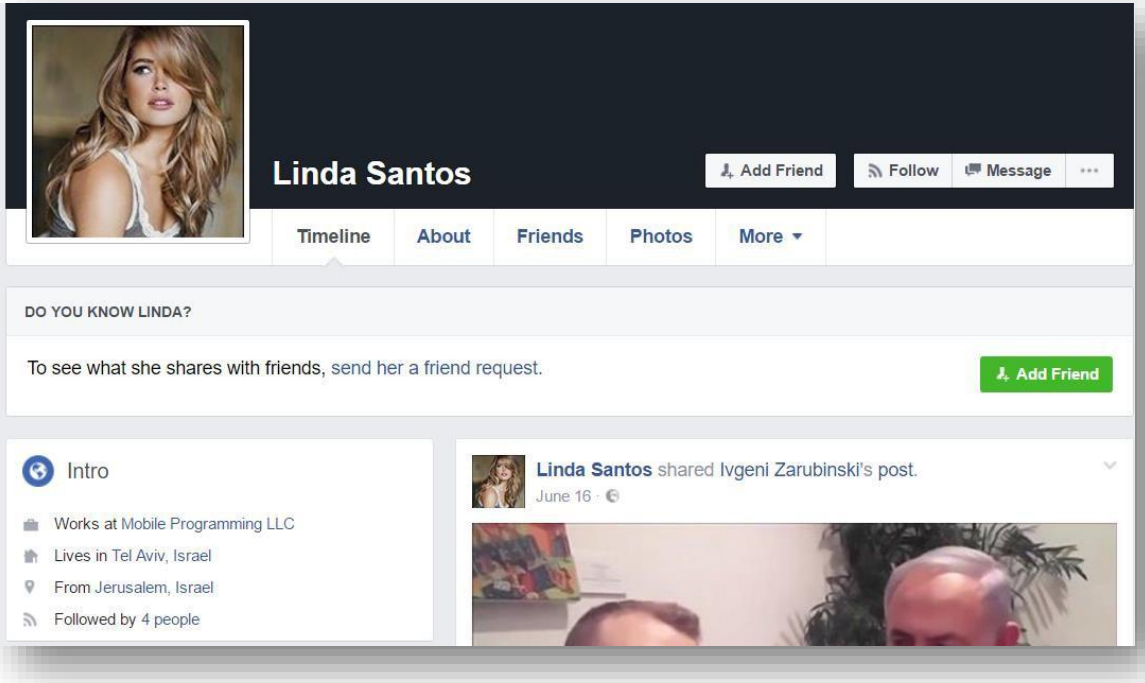
Guten Tag

2 Flugtickets wurden auf Ihren Namen gebucht.
Sie finden bezahlte Fahrkarten im Attachment.

Das zu Melani gehörende Computer Emergeny Response Team des Bundes (GovCERT) warnt auf Twitter vor E-Mails in Namen der Fluggesellschaft «Swiss». Im Anhang befinde sich der E-Banking-Trojaner Retefe. Schon im letzten Jahr waren viele Phishing-Mails mit dem Trojaner im Umlauf

- Mit Phishing wird versucht Informationen zu stehlen
- Typischerweise wird versucht an die Login-Daten von Mailaccounts, Cloud-Diensten, E-Banking-Accounts etc. zu gelangen
- Technisch gesehen ist Phishing KEIN HACKING

Aktuelle Bedrohungslage: Social Engineering



- Zwischen 2016 und 2017 versuchten unbekannte Täter die «Israel Electric Company» anzugreifen
- Der Angriff erfolgte indirekt: Es wurde versucht Geräte von Mitarbeitenden zu infizieren (auch private Geräte)
- Unter anderem tauchte das falsche Facebook-Profil «Linda Santos» auf, welche mit mehreren Mitarbeitenden von IEC in Kontakt trat

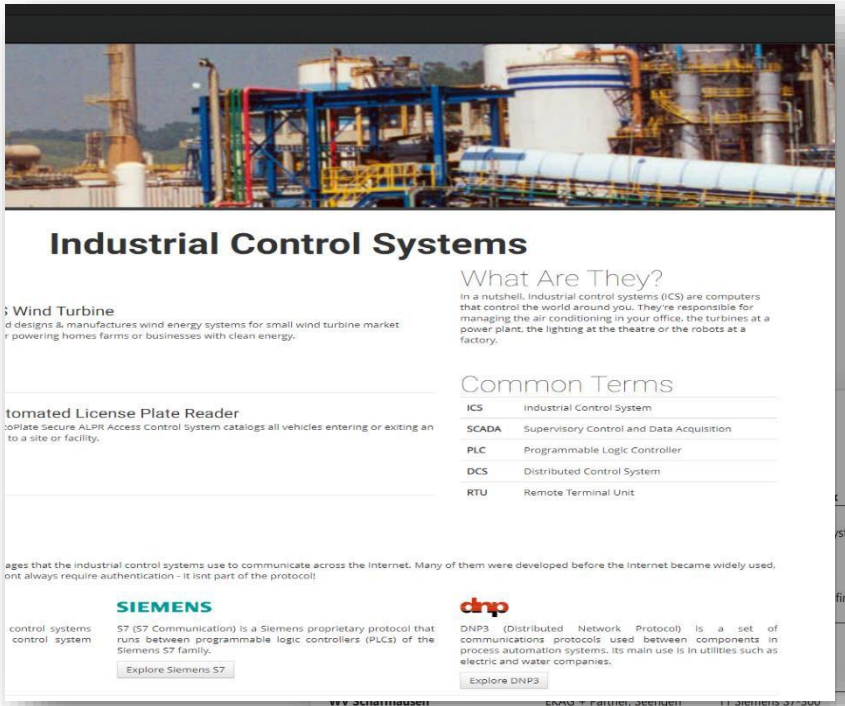
Aktuelle Bedrohungslage: Social Engineering

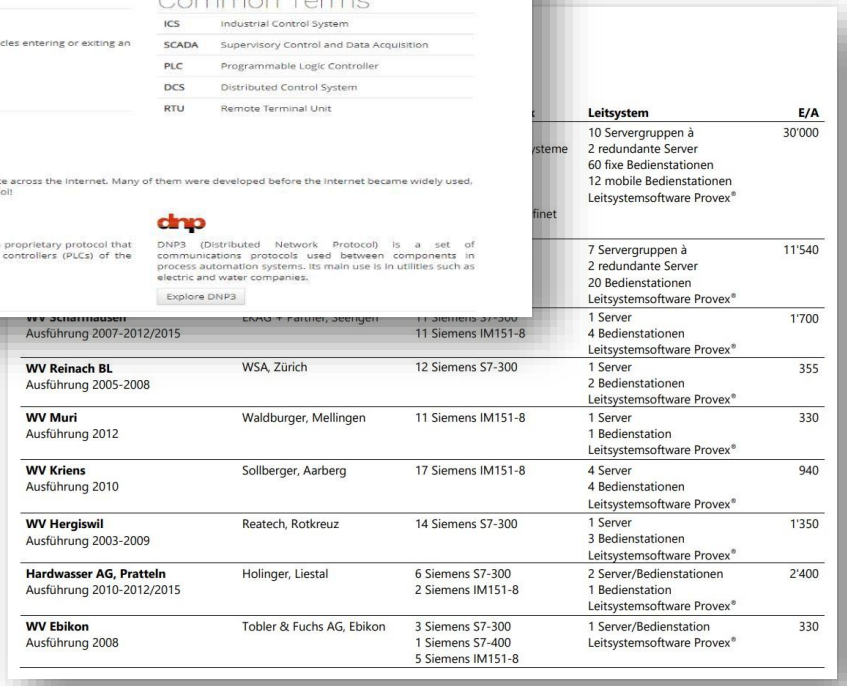
- «Linda» gewann einige Freunde bei der IEC…
- Transparenz kann auch missbraucht werden!

Aktuelle Bedrohungslage: Social Engineering / Hacking

- Metall Zug (ehemals V-Zug) wurde 2020 Opfer eines mehrstufigen Angriffs von Cyberkriminellen
- Zuerst wurde das E-Mail Konto eines Mitarbeitenden gehackt
- Durch das Mitlesen der Mails erfuhren die Kriminellen von geplanten Banküberweisungen
- Es gelang ihnen, sich glaubwürdig in die Mail-Kommunikation einzuschalten und den Mitarbeitenden davon zu überzeugen, das Geld auf eine andere Kontonummer zu überweisen
- Metall Zug entstand ein Schaden von ca. 2.5 Millionen CHF

Shodan.io «Die gefährlichste Webseite der Welt»





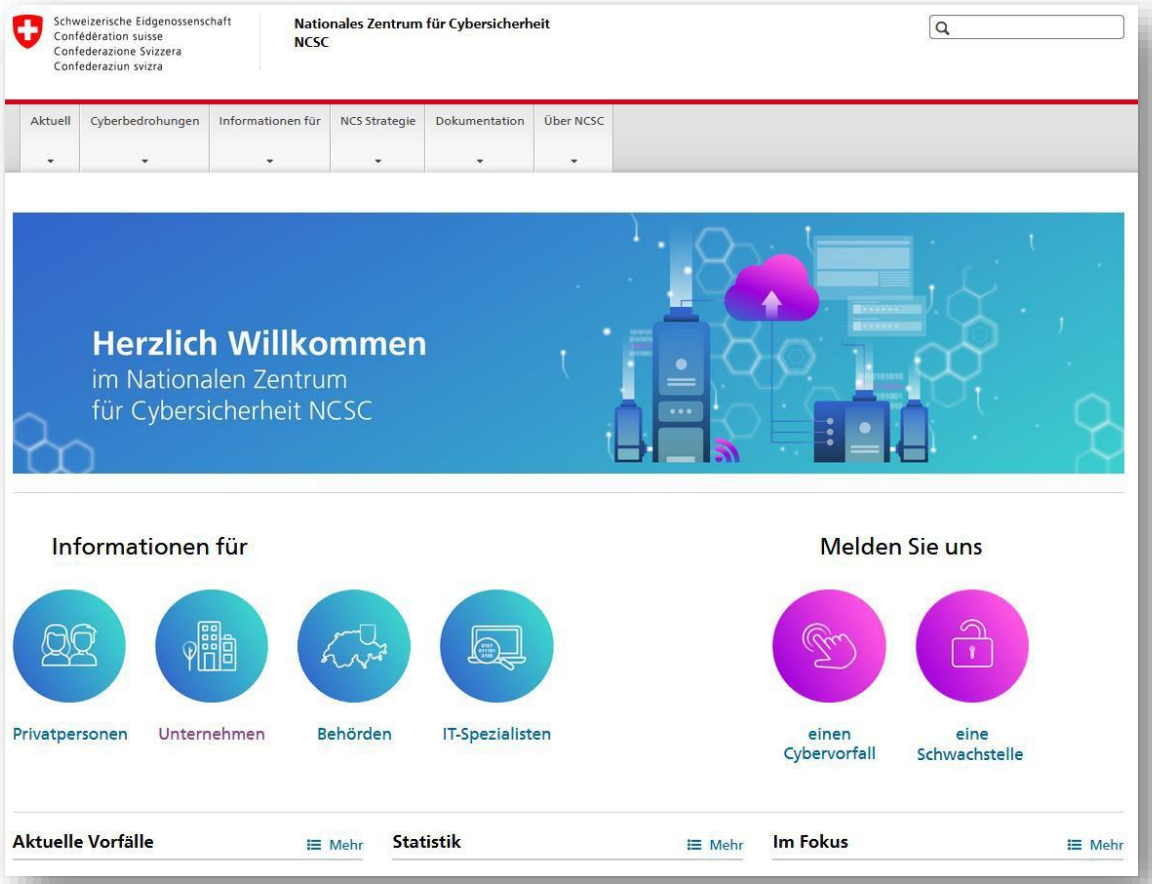
			Leitsystem	E/A
			10 Servergruppen à 2 redundante Server 60 fixe Bedienstationen 12 mobile Bedienstationen Leitsystemsoftware Provex®	30'000
			7 Servergruppen à 2 redundante Server 20 Bedienstationen Leitsystemsoftware Provex®	11'540
		11 Siemens IM151-8	1 Server 4 Bedienstationen Leitsystemsoftware Provex®	1'700
WV Reinach BL Ausführung 2005-2008	WSA, Zürich	12 Siemens S7-300	1 Server 2 Bedienstationen Leitsystemsoftware Provex®	355
WV Muri Ausführung 2012	Waldburger, Mellingen	11 Siemens IM151-8	1 Server 1 Bedienstation Leitsystemsoftware Provex®	330
WV Kriens Ausführung 2010	Sollberger, Aarberg	17 Siemens IM151-8	4 Server 4 Bedienstationen Leitsystemsoftware Provex®	940
WV Hergiswil Ausführung 2003-2009	Reatech, Rotkreuz	14 Siemens S7-300	1 Server 3 Bedienstationen Leitsystemsoftware Provex®	1'350
Hardwasser AG, Pratteln Ausführung 2010-2012/2015	Holinger, Liestal	6 Siemens S7-300 2 Siemens IM151-8	2 Server/Bedienstationen 1 Bedienstation Leitsystemsoftware Provex®	2'400
WV Ebikon Ausführung 2008	Tobler & Fuchs AG, Ebikon	3 Siemens S7-300 1 Siemens S7-400 5 Siemens IM151-8	1 Server/Bedienstation Leitsystemsoftware Provex®	330

- Shodan.io ist eine Webseite, die wie Google funktioniert
- Man findet damit aber nicht Dokumente / Informationen, sondern am Internet angeschlossene Geräte (IoT)
- Macht es Angreiffern sehr einfach, potenzielle Ziele auszukundschaften
- Sind Ihre Geräte auf Shodan.io sichtbar, haben Sie ein potenzielles Sicherheitsproblem!
- Über Shodan lassen sich z.B. DICOM-Bildserver suchen

Hausaufgaben (Auswahl)

Identifizieren	Identifizieren und dokumentieren Sie Ihre Geschäftsprozesse (Business Continuity Mgmt) Dokumentieren Sie all Ihre IKT-Systeme, Dienste, Prozesse, Berechtigungen, Lizenzen, etc. Bewerten Sie Ihre IKT-Risiken im unternehmensweiten Riskmanagement
Schützen	Verwenden Sie Schutztechnologien (Antivirus, Firewall, Intrusion-Detection, etc.) Definieren Sie Richtlinien (z.B. Umgang mit Passwörtern, Einsatz privater Geräte) Schulen Sie Ihre Mitarbeiter und führen Sie Übungen oder Penetration-Tests durch
Erkennen	Dokumentieren Sie die «Baseline» Ihrer Informatikprozesse (z.B. Datenflüsse) Schulen Sie Ihre Mitarbeitenden darin, Abweichungen vom Normalzustand zu erkennen Verwenden Sie technische Detektionsmethoden (z.B. Heuristische Methoden oder KI)
Reagieren	Entwickeln Sie verschiedene Risikoszenarien gemäss Ihrem Riskmanagement (z.B. Szenario DDOS, Szenario APT, Verletzung der Datenintegrität, etc.) Definieren Sie präzise Reaktionspläne nach dem Prinzip «Wer tut was, wann und wieso?»
Wiederherstellen	Stellen Sie sicher, dass Ihre kritischen Systeme georedundant betrieben werden Etablieren Sie einen Backup/Restore-Prozess der höchsten Anforderungen genügt Führen Sie min. 1x jährlich einen kompletten Restore auf den produktiven Systemen durch

Angebote des Bundes: Unterstützung durch das NCSC

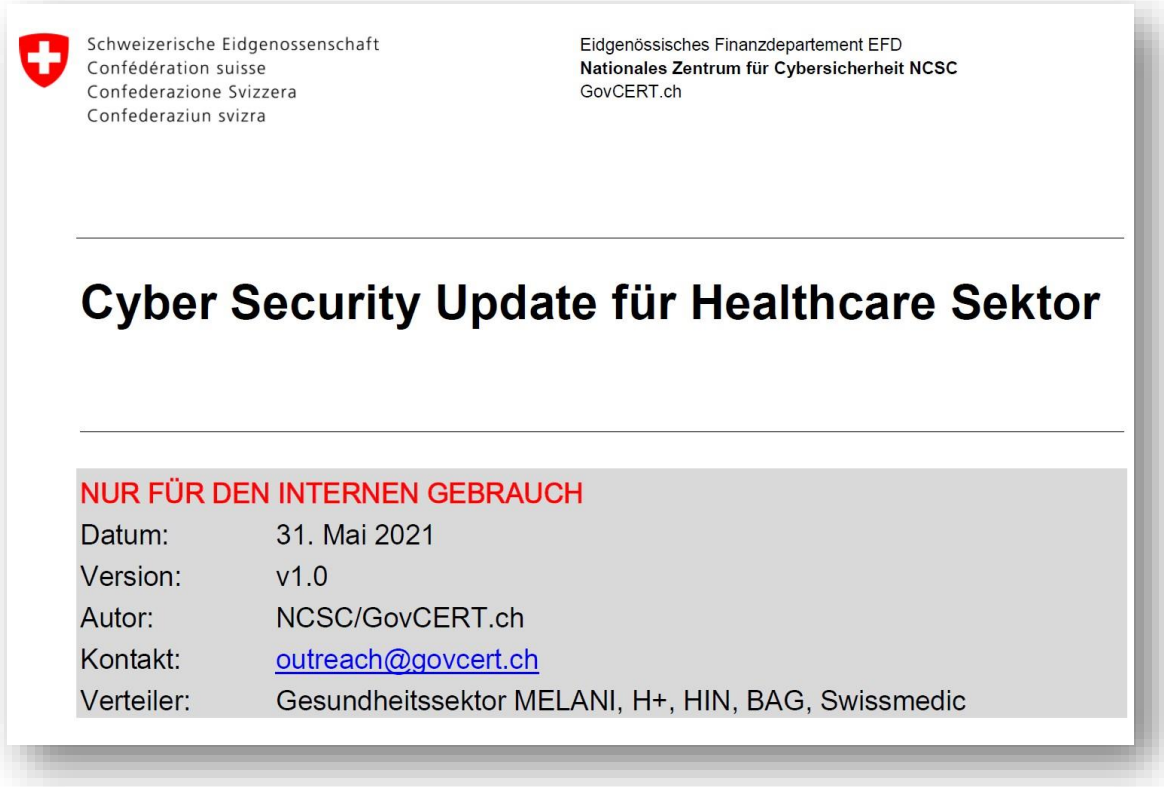


- GovCERT, hat technische Hilfsmittel entwickelt, die Angriffsversuche von bekannten kriminellen Netzwerken automatisch blockieren.
- Diese Hilfsmittel können die Spitäler gratis beim NCSC beziehen und mit wenig Aufwand einsetzen.
- Über die «geschlossenen Kundenkreise», sowie die Austauschplattform der Melde- und Analysestelle Informationssicherung (MELANI) fördert das NCSC den Informations- und Wissensaustausch im Gesundheitssektor.

www.ncsc.admin.ch

Kontakt: outreach@govcert.ch
ncsc@gsefd.admin.ch

Angebote des Bundes: Cyber Security Update



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Nationales Zentrum für Cybersicherheit NCSC
GovCERT.ch

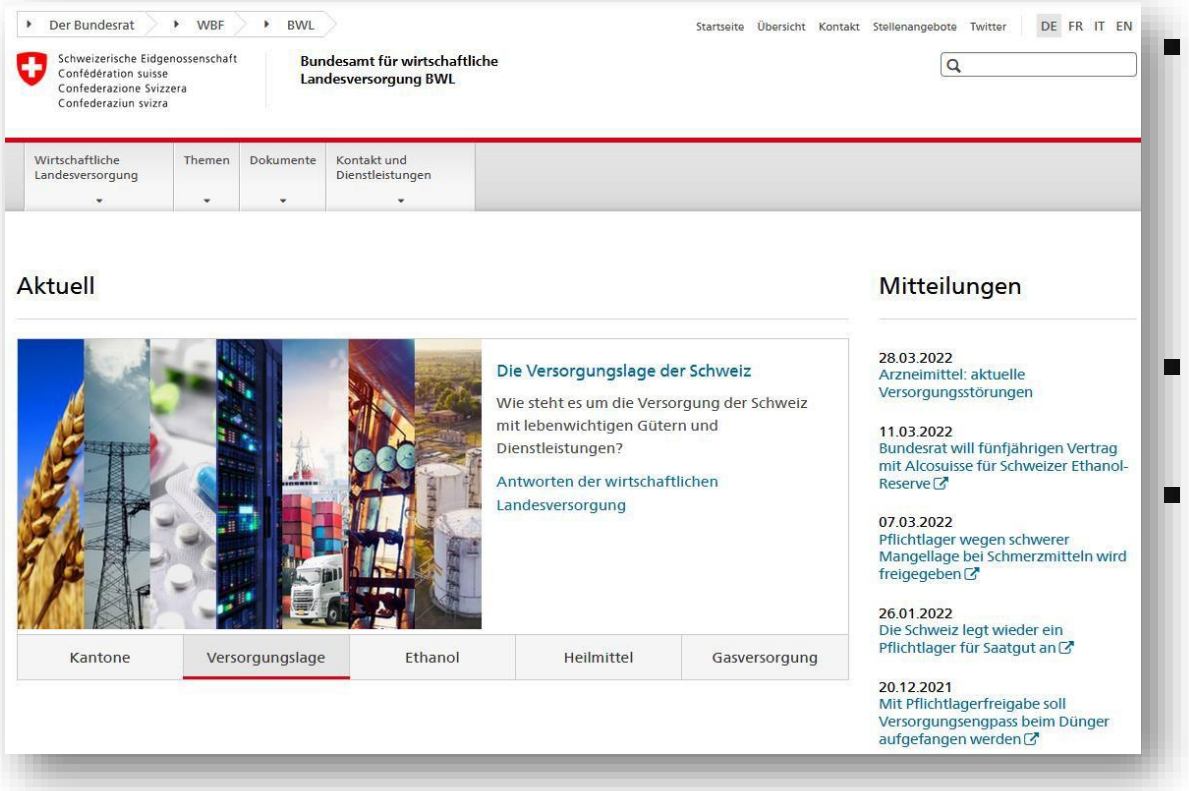
Cyber Security Update für Healthcare Sektor

NUR FÜR DEN INTERNEN GEBRAUCH

Datum:	31. Mai 2021
Version:	v1.0
Autor:	NCSC/GovCERT.ch
Kontakt:	outreach@govcert.ch
Verteiler:	Gesundheitssektor MELANI, H+, HIN, BAG, Swissmedic

- GovCERT publiziert regelmässig Updates zur Cybersecurity für spezifische Branchen.
- Die Mitglieder im «Geschlossenen Kundenkreis Gesundheitssektor» bei MELANI (NCSC) werden über diesen Kanal laufend über aktuelle Entwicklungen, Erkenntnisse und Bedrohungen informiert.
- Diese Informationen sind klassifiziert und nur für Mitglieder zugänglich.

Angebote des Bundes: Abteilung Gesundheitswesen BWL



- Der Fachbereich IKT im Bundesamt für wirtschaftliche Landesversorgung BWL ist für die Verbesserung der Resilienz der kritischen Versorgungs-Infrastrukturen gegenüber Cyberrisiken verantwortlich.
- Massnahmen «Aus der Branche, für die Branche»
- Aktuell in Arbeit: IKT Minimalstandard Gesundheitswesen

Aktuelle Mitglieder

- Michel Buri Hôpital Valais *(Abteilungsleiter)*
- Erik Dinkel *Unispital Zürich (Stv. Abteilungsleiter)*
- Stefanie Rufinatscha *Triemlispital*
- Dr. Stefan Hunziker, *LUKS*
- Isabelle Udriot *CHUV*
- Franck Calcavecchia *HUG*
- Philipp Stoll *UKKB*
- Werner Ulmer *KSSG*
- Michele Marazza *EOC*
- *Stefan Juon KSGR*

www.bwl.admin.ch
daniel.caduff@bwl.admin.ch

Kontakt

Bundesamt für wirtschaftliche Landesversorgung BWL

Bernastrasse 28
3003 Bern
Tel. +41 58 462 21 71

Daniel Caduff
Stv. Leiter Geschäftstelle IKT
daniel.caduff@bwl.admin.ch