Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'économie, de la formation et de la recherche WBF

Office fédéral pour l'approvisionnement économique du pays OFAE Domaine TIC

Les cyber-risques dans les hôpitaux

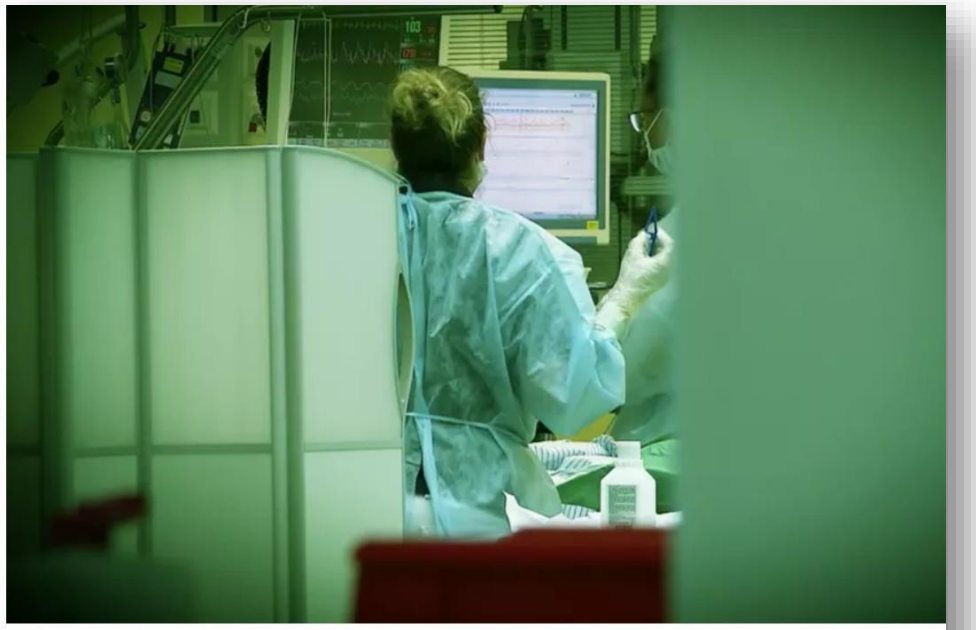
Situation actuelle et mesures recommandées

Daniel Caduff
Office fédéral pour l'approvisionnement économique du pays OFAE
Suppléant du chef du bureau TIC

Hôpitaux : des défis particuliers

- Contrairement à d'autres infrastructures critiques, les hôpitaux sont accessibles et ouverts à tous.
- Il existe des systèmes, comme les machines cardio-pulmonaires, pour lesquels les cyber-attaques sont potentiellement mortelles.
- Un hôpital a parfois des centaines d'appareils provenant de différents fabricants en service -> il est donc extrêmement difficile de gérer l'entretien et de garder la vue d'ensemble.
- La certification des appareils médicaux interdit la modification ultérieure du logiciel -> il n’est pas possible d’effectuer les mises à jour correctement.
- Dans les hôpitaux, les systèmes critiques sont gérés par les médecins et le personnel soignant -> pas par des spécialistes cyber

Hôpitaux : cyberattaque contre Hôpital de 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.

- L'hôpital de Wetzikon a été victime d'une attaque de ransomware en 2019 (EMOTET comme dropper)
- Plusieurs appareils médicaux ont dû être mis temporairement hors service.
- L'attaque a été rapidement identifiée et a pu être contenue efficacement.
- Mais :
  - Les médecins n'avaient pas accès aux dossiers des patients.
  - Des opérations ont dû être reportées.
  - Des études n'ont pas pu être menées.

Exemple : cyberattaque du groupe Hirslanden

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

- En juillet 2020, le groupe Hirslanden a été infecté par le logiciel malveillant "Trickbot"
- L'affaire n'a été rendue publique que fin 2020.
- Selon le groupe Hirslanden, les pirates ont réussi à atteindre les composants centraux du réseau ainsi que les serveurs.
- Aucune donnée n'a été volée.
- De même, aucune donnée de patient n'aurait été cryptée, mais uniquement des documents administratifs.
- Tous les fichiers ont pu être restaurés grâce aux sauvegardes.
- Le préjuidice a duré 6 jours.

Exemple : cyberattaque des cliniques Pallas

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.

- En août 2021, le groupe de cliniques privées "Pallas Kliniken" a été victime d'une attaque par *ransomeware*.
- Plusieurs systèmes informatiques n'étaient alors plus disponibles. Afin d'éviter une propagation, les systèmes ont été arrêtés de manière contrôlée.
- Plusieurs traitements prévus n'ont pas pu être réalisés et certains patients ont dû être renvoyés chez eux.

Sécurité vs. sûreté

- *Safety* = sécurité des vies humaines
- *Security* = sécurité de l'information
- La *Safety* passe toujours avant la *Security*

- Les cyber-risques peuvent être à la fois liés à la *Safety* et à la *Security*.

- Les violations de la protection des données sont pertinentes pour la *Security*, mais pas pour la *Safety*.

- Les attaques contre les systèmes TIC d'appareils phyisiques (p. ex. IRM, respirateur, appareil de dialyse) sont potentiellement mortelles pour les patients et donc importantes pour la *Safety* !

- La disponibilité passe avant la protection des données !

Stratégie de protection de la Suisse contre les cyber-risques NCS

- En 2012, le Conseil fédéral a adopté la "Stratégie nationale pour la protection de la Suisse contre les cyberrisques" (SNPC).
- L'OFAE a développé des normes minimales TIC sectorielles en collaboration avec différentes associations faîtières.
- La norme minimale TIC (générale) est une mesure préventive visant à renforcer la résilience des TIC au sens de la SNPC.
- La norme minimale TIC sectorielle pour les hôpitaux est actuellement en cours d'élaboration.

Répartition des tâches Cyber au sein de la Confédération

Cyberdéfense
DDPS

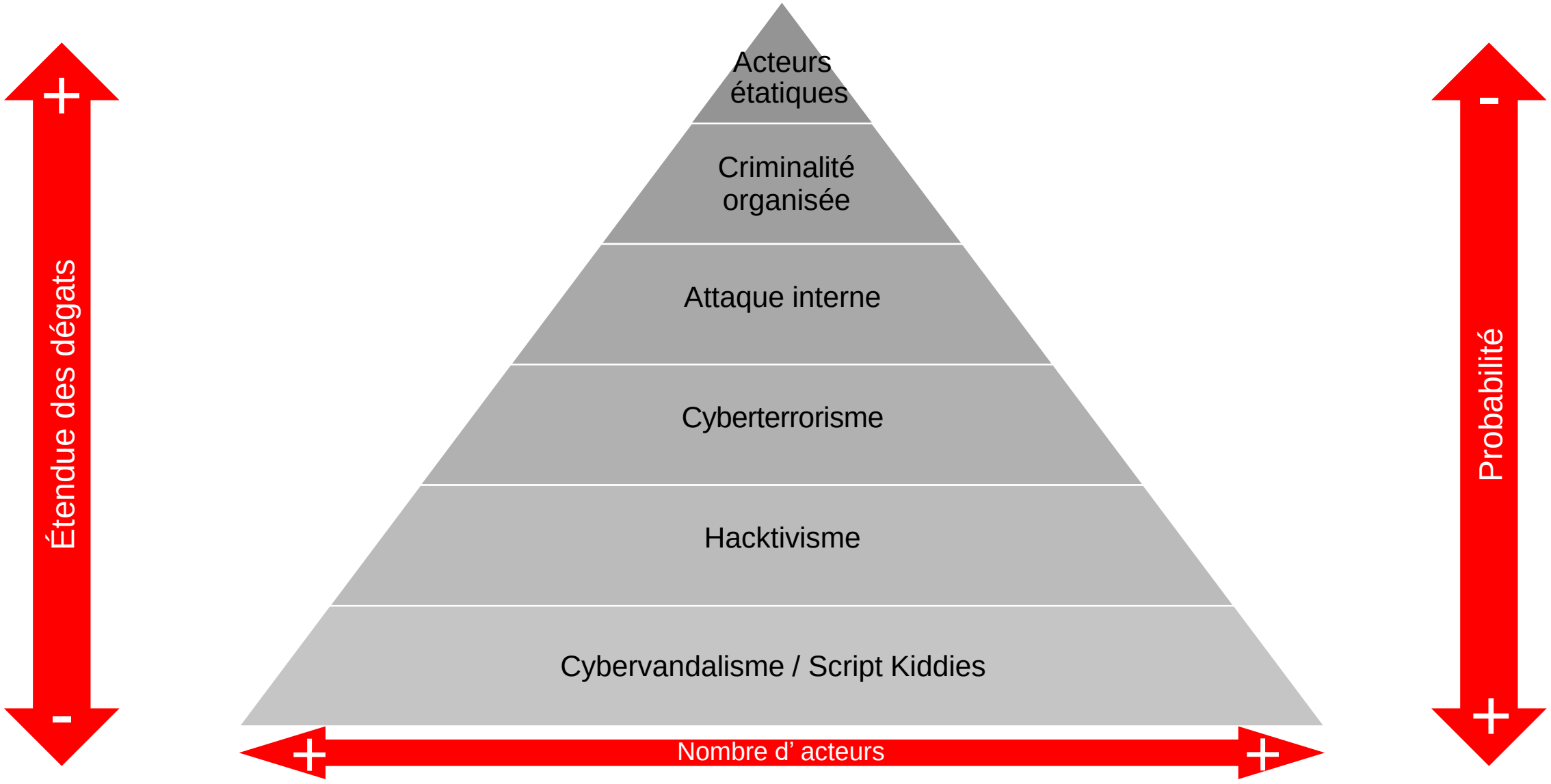
Cybercriminalité
DFJP

Cybersécurité
DEFR / DFF / DFAE

tâches :

- Défense (cyberdéfense)
- Application de la loi (cybercriminalité)
- Protection des infrastructures critiques (cybersécurité)
- Séparation organisationnelle, mais collaboration étroite et concertation mutuelle.

Pyramide des Cyber-risques



Norme minimale TIC

- La norme est universelle
- L'accent est mis en premier lieu sur les infrastructures critiques
- La norme indique *ce qu'il* faut faire, mais laisse à l'utilisateur la liberté de décider *comment* il veut le faire
- La norme est compatible avec les normes industrielles internationales, telles que les normes ISO

Lien de téléchargement des normes et des outils

Objectifs de la norme

- La cybersécurité, comprend la confidentialité, l'intégrité et la disponibilité des données.
- Avec la norme minimale TIC, l‘OFAE met à la disposition des entreprises un outil polyvalent.

Confidentialité

- Données des patients
- Données personnelles
- Comptabilité
- ...

-> en partie des prescriptions légales, mais **non pertinentes pour la safety.**

Intégrité

- Données des patients
- Données laboratoire
- Valeurs de mesure

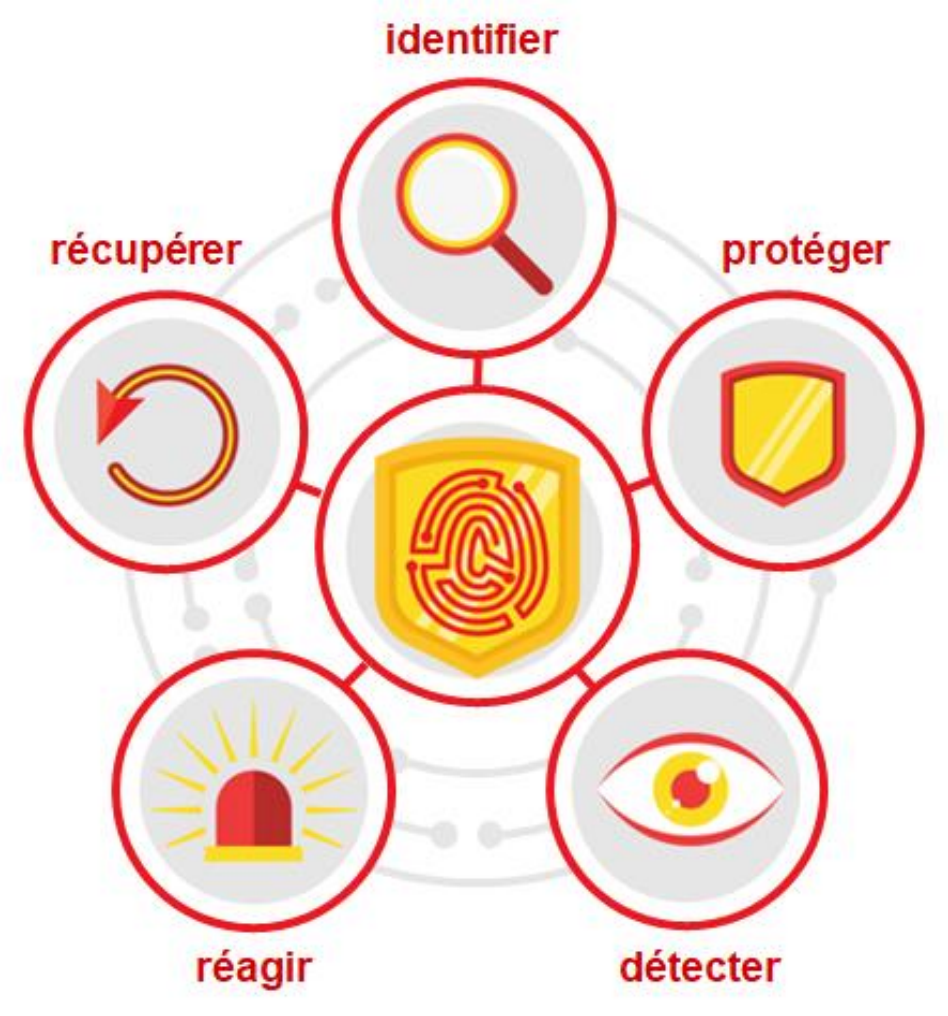
-> des valeurs de mesures ou des données de laboratoires erronées peuvent entraîner des erreurs de traitements.
-> **Pertinent pour la Safety !**

Disponibilité

- Systèmes d’information des patients
- Systèmes TIC d’appareils physiques

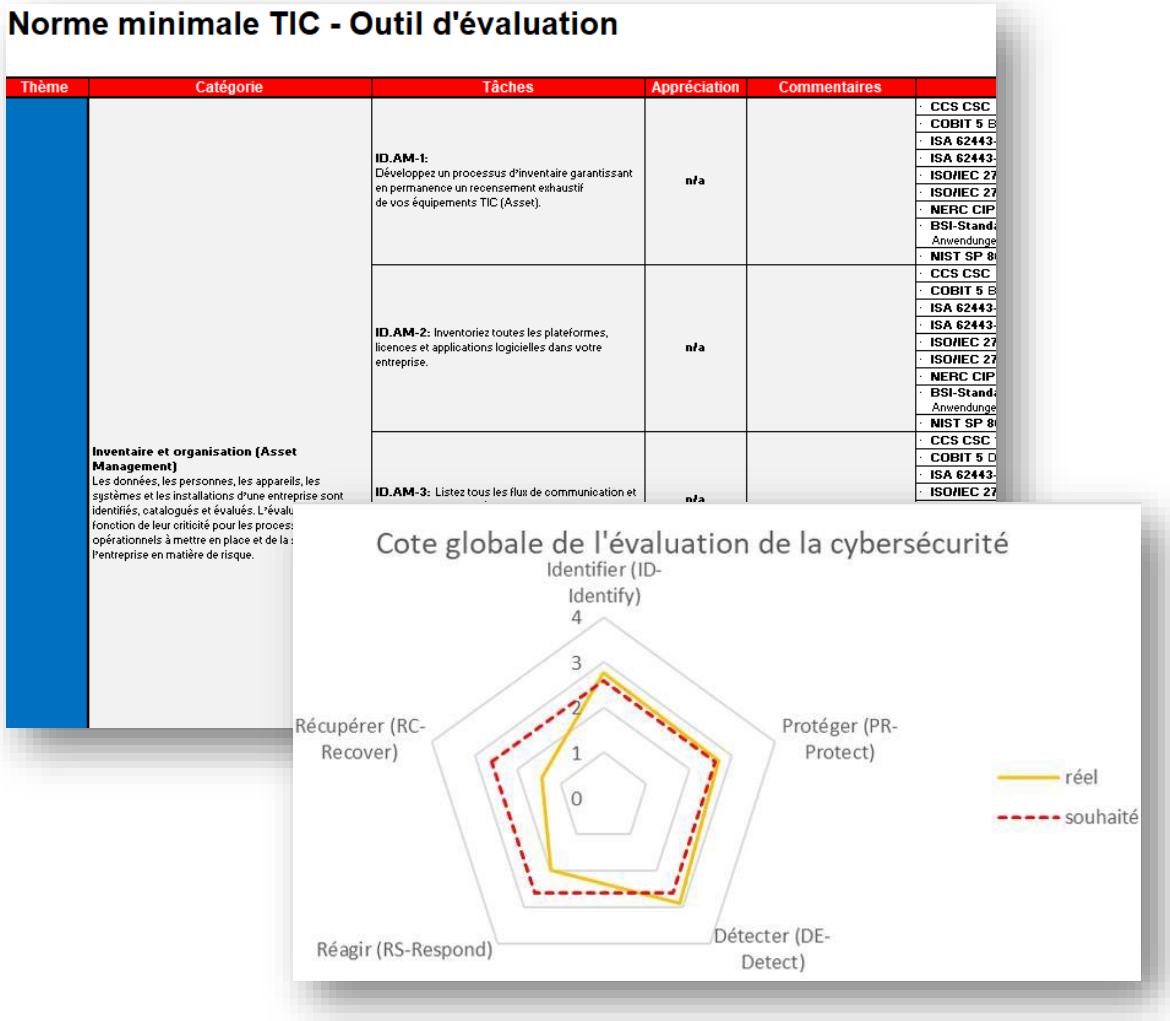
-> La manipulation ou la défaillance d'une machine cardio-pulmonaire est potentiellement mortelle.
-> **Pertinent pour la Safety !**

Comment fonctionne la norme ?



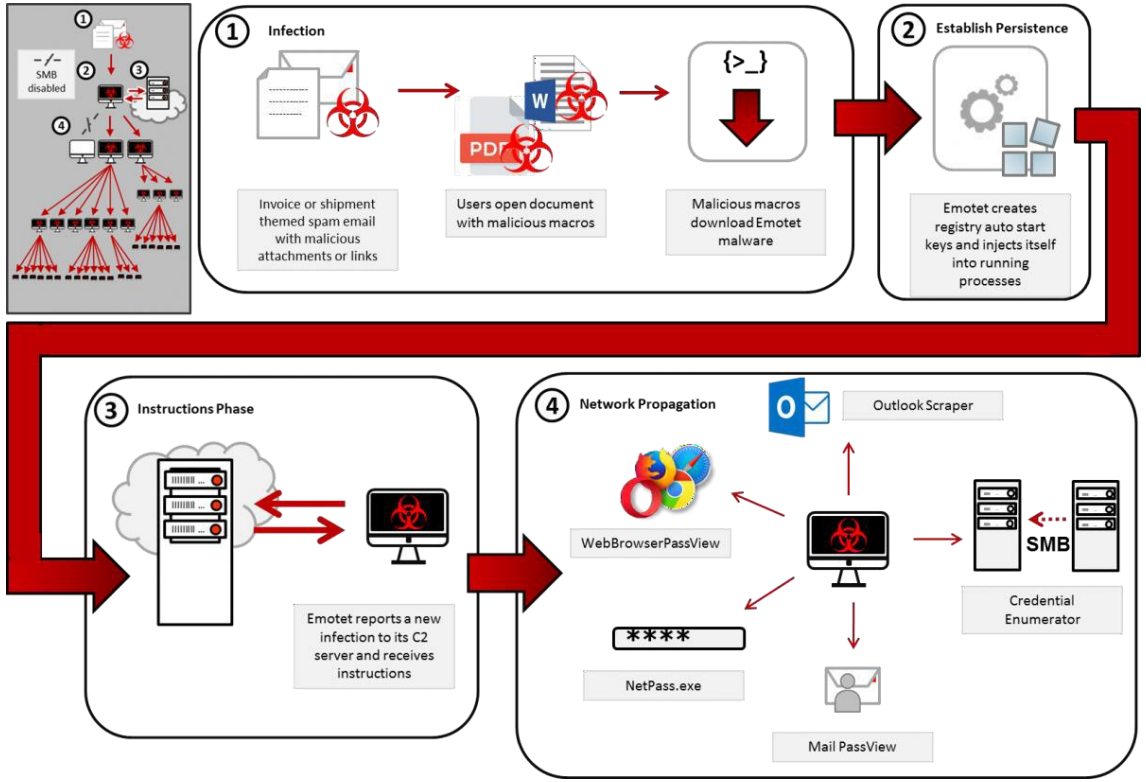
- La norme a été développée par les experts de l'approvisionnement économique du pays et s'articule autour de 5 chapitres.
- Pour chaque chapitre, la norme recommande des activités spécifiques.
- Au total, il s'agit de 106 activités dont la mise en œuvre est évaluée de 0 à 4.

Comment fonctionne la norme ?



- Pour la mise en œuvre, la Confédération met à disposition un outil Excel.
- L'évaluation des 106 activités permet à l'utilisateur d'évaluer son niveau de protection.
- La norme est basée sur les risques et peut être auditée.

Menaces actuelles : ransomware
EMOTET / Trickbot / Ryuk



- EMOTET est un malware qui est souvent distribué par e-mail
- EMOTET se propage ensuite de manière indépendante, par exemple en copiant toutes les adresses électroniques qu'il peut trouver.
- EMOTET peut transporter un arsenal différent d'outils selon les besoins. Actuellement, par exemple, il s'agit souvent du logiciel de rançon "Ryuk" ou du cheval de Troie de la banque en ligne "Trickbot".
- EMOTET a également attaqué avec succès des entreprises suisses : Meier Tobler, Offix, Lobsinger Marazzi et l'hôpital de Wetzikon !
- Victimes internationales : entre autres la Cour d'appel de Berlin, et plusieurs administrations municipales américaines !

Menaces actuelles : ransomware "WannaCry"

- Se propage de manière autonome sous forme de ver
- Exploite une faille connue depuis longtemps dans Windows XP
- Responsable de la panne de plusieurs infrastructures critiques, en particulier d'hôpitaux au Royaume-Uni.
- De nombreux particuliers et entreprises perdent des données
- Chiffre d'affaires estimé : environ 50 millions USD

Attaques de ransomware réussies en Suisse

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.

- Seulement une sélection d'attaques réussies ("pointe de l'iceberg")
- Tous les types d'entreprises peuvent être concernés
- Infrastructures critiques également touchées (notamment l'hôpital de 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

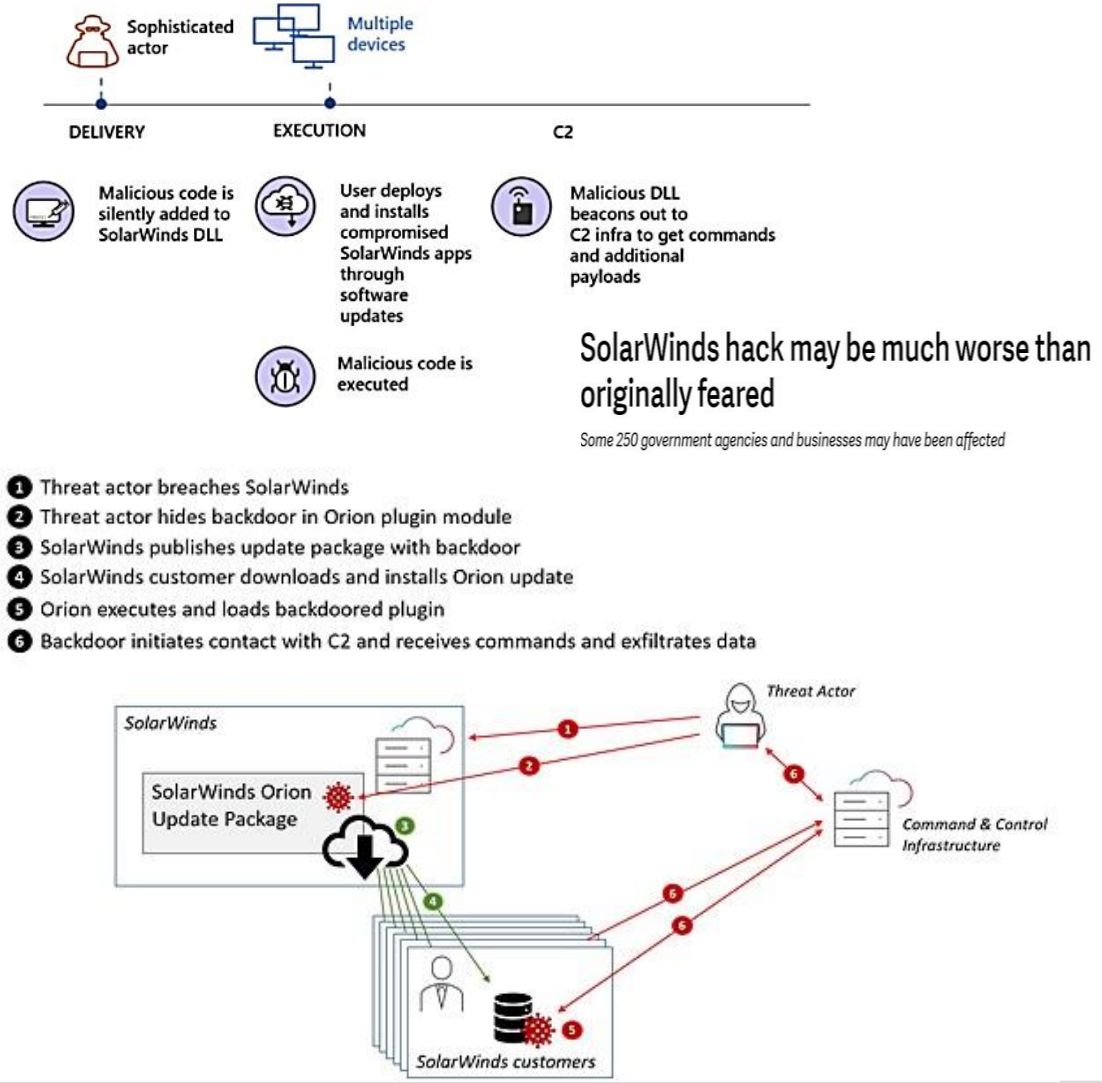
Das Ransomware-Trio Emotet, Trickbot und Ryuk hat die IT-Systeme der Offix-Gruppe lahmgelegt. CEO Martin Kelterborn erklärt den Ablauf des Hackerangriffs im Gespräch mit inside-it.ch

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.

Menaces actuelles : attaque de la chaîne d'approvisionnement Solar Wind hack sur Fire Eye



- SolarWinds est une grande entreprise informatique qui propose des logiciels aux institutions allant des entreprises du classement "Fortune 500" au gouvernement américain.
- L'attaque n'a pas été détectée pendant des mois et aurait pu exposer des données aux plus hauts niveaux du gouvernement, y compris l'armée américaine et la Maison Blanche.
- Une mise à jour contenant un *malware* a fait jusqu'à 18 000 victimes parmi les organisations.
- La mise à jour était censée combler une faille de sécurité.
- ampleur des dommages pouvant atteindre 100 milliards de dollars US.

Menaces actuelles : DDOS

de fr it

Zürich 18°

Schweiz Ausland Wirtschaft Sport People Entertainment Digital Wisse

News E-Spor

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.

- Simple mais efficace
- Les serveurs sont submergés de demandes concentrées jusqu'à ce qu'ils ne puissent plus résister à l'assaut.
- Aujourd'hui, cela peut être loué comme service illégal ("Hacking as a Service")

Menaces actuelles : 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

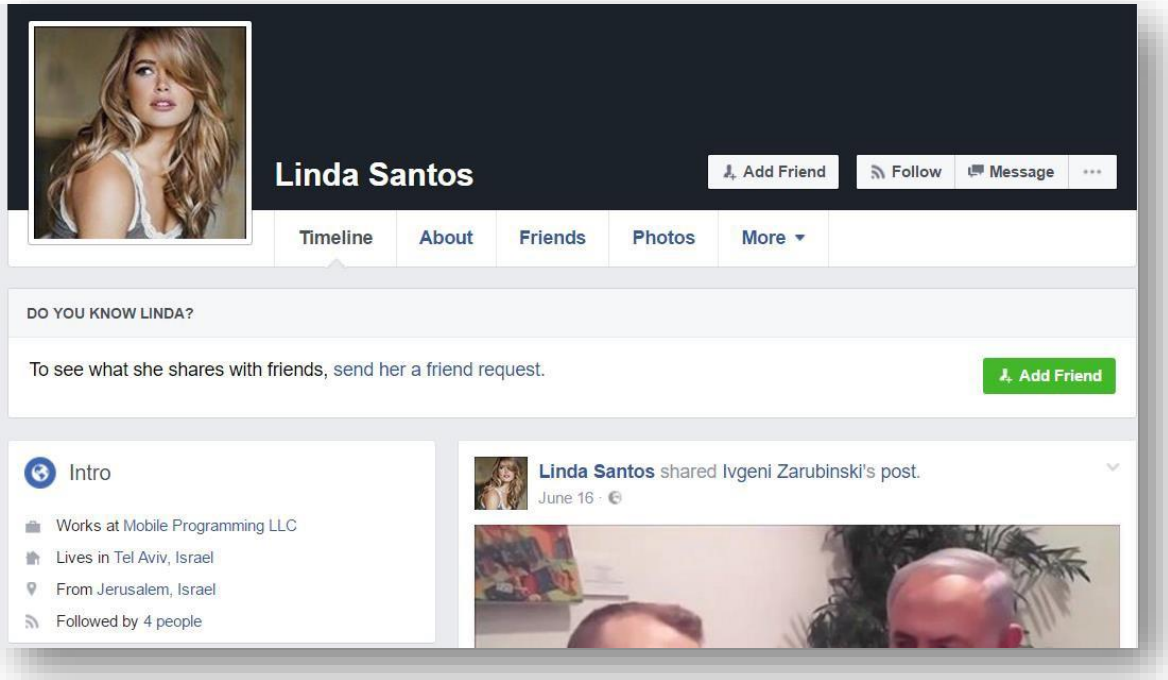
Guten Tag

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

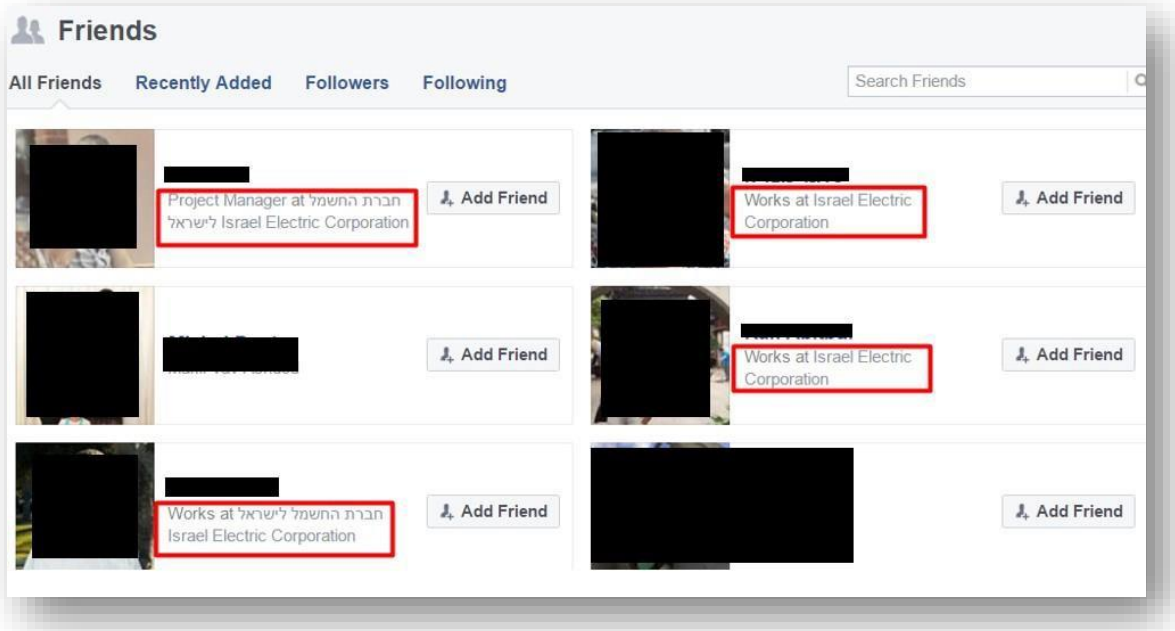
- Le phishing est une tentative de vol d'informations
- Il s'agit typiquement d'une tentative d'accès aux données de connexion des comptes de messagerie, des services de cloud, des comptes bancaires électroniques, etc.
- Techniquement, le phishing n'est PAS du HACKING

Menaces actuelles : l'ingénierie sociale



- Entre 2016 et 2017, des inconnus ont tenté d'attaquer la "Israel Electric Company".
- L'attaque a été indirecte : on a tenté d'infecter les appareils des collaborateurs (y compris les appareils privés).
- Entre autres, le faux profil Facebook de "Linda Santos" est apparu, qui a pris contact avec plusieurs collaborateurs d'IEC.

Menaces actuelles : l'ingénierie sociale

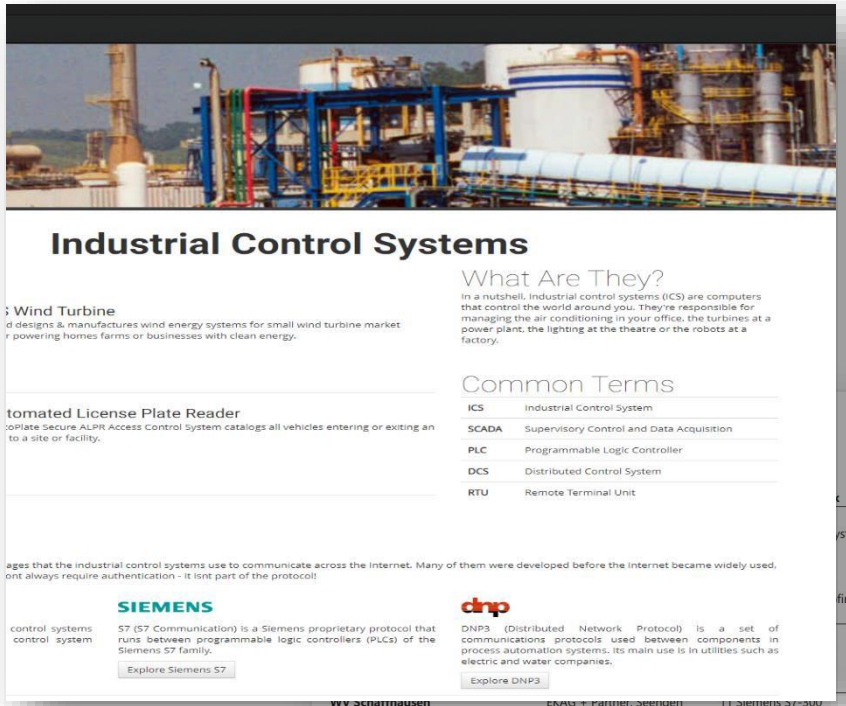


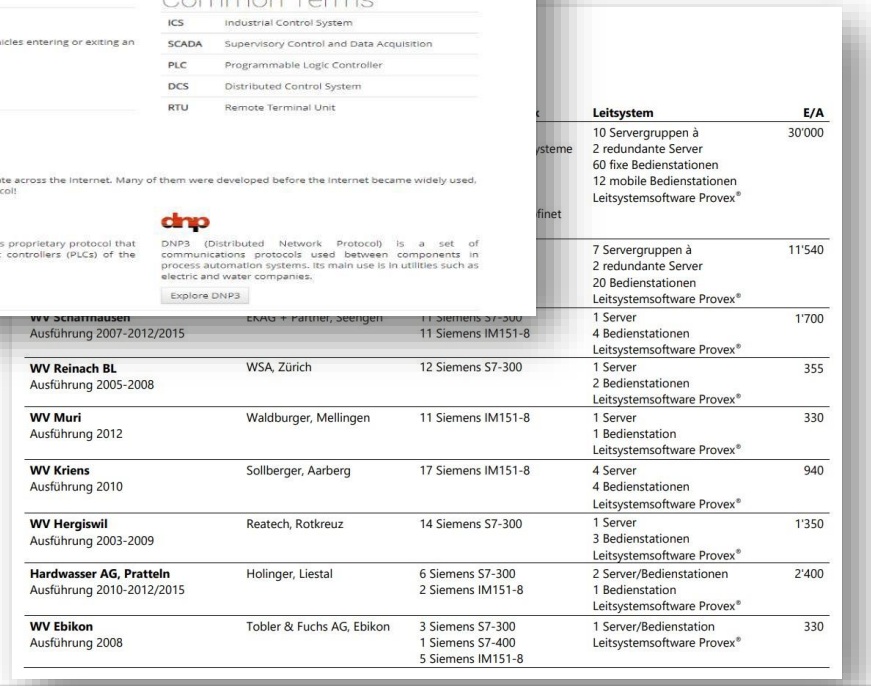
- "Linda" s'est fait quelques amis à l'IEC
- La transparence peut aussi être utilisée à mauvais escient !

Menaces actuelles : ingénierie sociale / piratage informatique

- En 2020, Metall Zug (anciennement V-Zug) a été victime d'une attaque à plusieurs niveaux de la part de cybercriminels
- D'abord, le compte e-mail d'un employé a été piraté
- En lisant les e-mails, les criminels ont appris qu'il était prévu d'effectuer des virements bancaires.
- Ils ont réussi à s'impliquer de manière crédible dans la communication par e-mail et à convaincre le collaborateur de transférer l'argent sur un autre numéro de compte.
- Le train de métal a subi des dommages d'environ 2,5 millions de CHF

Shodan.io "Le site web le plus dangereux au monde





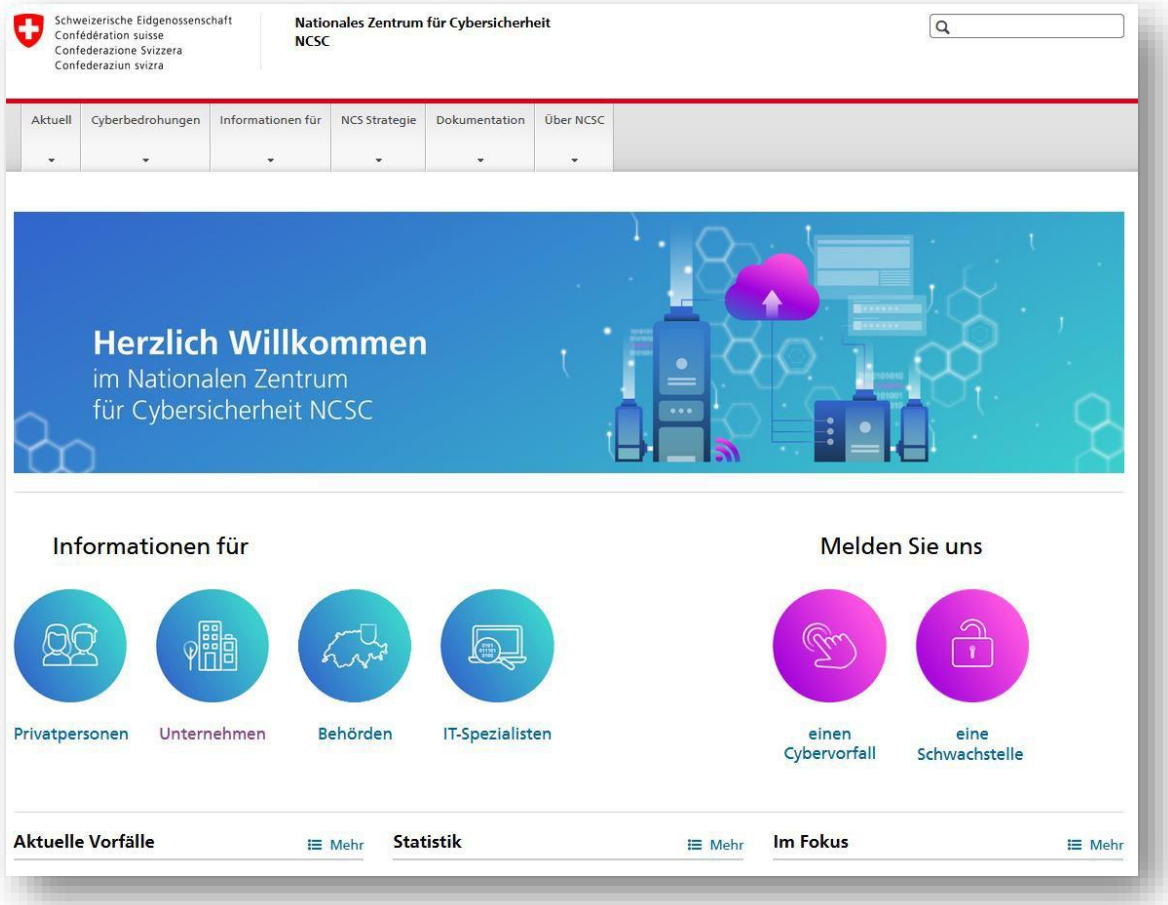
			Leitsystem	E/A
			10 Servergruppen à 2 redundante Server 60 fixe Bedienstationen 12 mobile Bedienstationen Leitsystemsoftware Provex®	30'000
			7 Servergruppen à 2 redundante Server 20 Bedienstationen Leitsystemsoftware Provex®	11'540
Ausführung 2007-2012/2015		11 Siemens IM151-8	1 Server 4 Bedienstationen 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 est un site qui fonctionne comme Google
- Il ne permet pas de trouver des documents/informations, mais des appareils connectés à Internet (IoT).
- Il permet aux attaquants de repérer facilement les cibles potentielles
- Si vos appareils sont visibles sur Shodan.io, vous avez potentiellement un problème de sécurité !
- Shodan permet de rechercher des serveurs d'images DICOM, par exemple.

Devoirs (choix)

Identifier	Identifiez et documentez vos processus d'entreprise (Business Continuity Mgmt). Documentez tous vos systèmes TIC, services, processus, autorisations, licences, etc. Évaluez vos risques TIC dans la gestion des risques de l'entreprise.
Protéger	Utilisez des technologies de protection (antivirus, pare-feu, détection d'intrusion, etc.). Définissez des directives (p. ex. utilisation de mots de passe, utilisation d'appareils privés). Formez vos collaborateurs et réalisez des exercices ou des tests d' intrusion.
Détecter	Documentez la "baseline" de vos processus informatiques (p.ex. flux de données). Formez vos collaborateurs à reconnaître les écarts par rapport à la situation normale. Utilisez des méthodes de détection techniques (p. ex. méthodes heuristiques ou IA).
Réagir	Développez différents scénarios de risque selon votre gestion des risques par ex scénario DDOS, scénario APT, violation de l'intégrité des données, etc.). Définir des plans de réaction précis selon le principe "qui fait quoi, quand et pourquoi ?".
Restaurer	Assurez-vous que vos systèmes critiques sont géo-redondants. Etablissez un processus de sauvegarde/restauration qui répond aux exigences les plus élevées. Effectuez au moins 1x par an une restauration complète sur les systèmes de production.

Offres de la Confédération : Soutien du NCSC

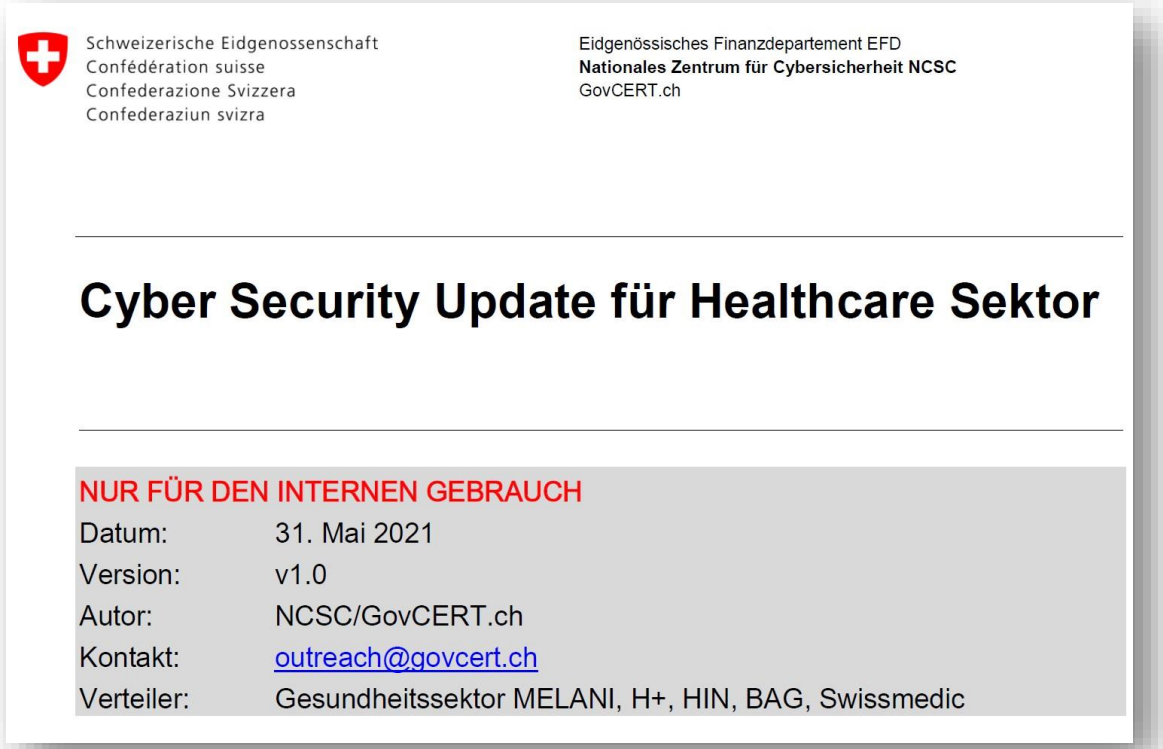


- GovCERT, a développé des outils techniques qui bloquent automatiquement les tentatives d'attaque de réseaux criminels connus.
- Les hôpitaux peuvent se procurer gratuitement ces outils auprès du NCSC et les utiliser avec un minimum d'efforts.
- Par le biais des "cercles fermés de clients", ainsi que de la plate-forme d'échange de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), le NCSC encourage l'échange d'informations et de connaissances dans le secteur de la santé.

www.ncsc.admin.ch

Contact :
- outreach@govcert.ch
- ncsc@gsefd. admin. ch

Offres de la Confédération : Mise à jour de la cybersécurité



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Nationales Zentrum für Cybersicherheit NCSC
GovCERT.ch

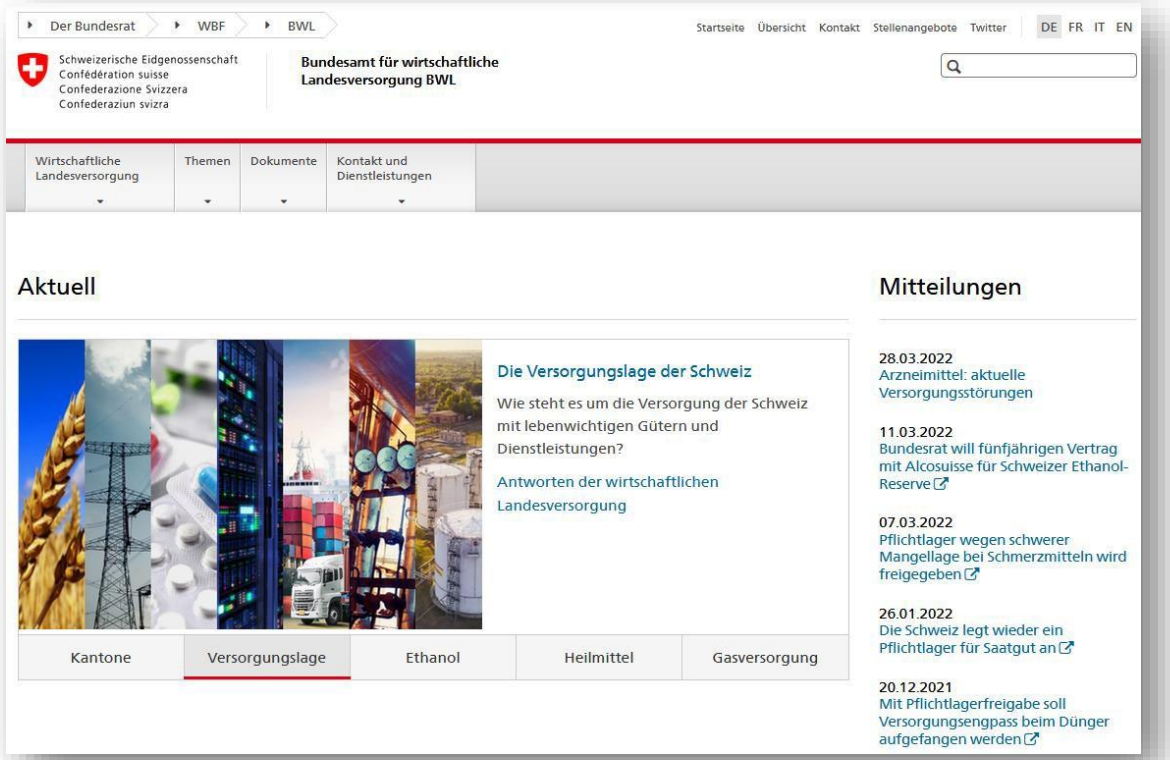
Cyber Security Update für Healthcare Sektor

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 publie régulièrement des mises à jour sur la Cybersécurité pour des secteurs spécifiques.
- Les membres du "cercle fermé des clients du secteur de la santé" auprès de MELANI (NCSC) sont informés en permanence par ce canal des évolutions, des découvertes et des menaces actuelles.
- Ces informations sont classifiées et accessibles uniquement aux membres.

Offres de la Confédération : Département de la santé publique OFAE



- La section TIC de l'Office fédéral pour l'approvisionnement économique du pays OFAE est chargée d'améliorer la résilience des infrastructures d'approvisionnement critiques face aux cyber-risques.
- Mesures "du secteur, pour le secteur»
- Actuellement en cours : norme minimale TIC pour la santé publique

Membres actuels

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

Site Internet de l'OFAE
daniel.caduff@bwl.admin.ch

Contact

Office fédéral pour l'approvisionnement économique du pays OFAE

Rue de Berne 28
3003 Berne
41 58 462 21 71

Daniel Caduff
Directeur adjoint du bureau TIC
daniel.caduff@bwl.admin.ch