SBB Inspiration Days – Die Zukunft beginnt heute.

Bern Wankdorf, 20.08.2024 bis 22.08.2024.

Ziel der SBB Inspiration Days.

- Präsentation zukunftsweisender, aktueller SBB-Projekte und Themen.
- Inspiration durch Externe.
- Förderung des Dialogs, der Vernetzung und der interdisziplinäreren Zusammenarbeit.
- Wissensvermittlung, Anregung zu Innovationen.
- Stärkung der "OneSBB"-Kultur.

SBB Inspiration Days werden präsentiert von UE-FIM.

Innovationsprojekte & Coaching

Methodisch gestützte Begleitung von Innovationsprojekten in Potentialevaluationen, sowie Problem- und Lösungsexplorationen.

Szenarien

Durch Szenarien zukünftige Chancen und Risiken proaktiv identifizieren und die Resilienz von Strategie- und Langfristplanungen fördern.

Koordination übergreifende Innovationen

Unternehmensweite Koordination von Innovationsprojekten.

Forschungs-& Hochschulzusammenarbeit

Koordination der SBB Forschungsgefässe, Koordination von Forschungsprojekten und Gewährleistung des Wissenstransfers in die SBB.

Community

SBB Community zur Stärkung der Innovationskultur und Synergienutzung im gesamten Unternehmen.

Workshop Facilitation

Gestaltung, Durchführung und Nachbereitung von Workshops zum Setup von Innovationsprojekten.

Data& Analytics

Quantitative Datenanalysen für die Unternehmensentwicklung.

Scouting& Innovationsnetzwerke

Weltweite Suche nach innovativen Lösungen und passenden Unternehmen sowie Pflege des SBB Innovationspartner Managements.

SBB Kickbox

Innovations- und Weiterbildungsprogramm für engagierte SBB Mitarbeitende mit guten Ideen.

innovation@sbb.ch

SBB CFF FFS

Cyber Abwehr bei der SBB

Andreas Meister, SBB IT, Cyber Solution Architekt
HS 2, 17.06.2024

No security breaches with damages or business impact

«Risiko Nummer eins für die SBB».

CEO-Survey von PwC

Schweizer CEOs sehen Cyberrisiken 2024 als Topbedrohung

Di 16.01.2024 - 17:46 Uhr
von Yannick Züllig und msc

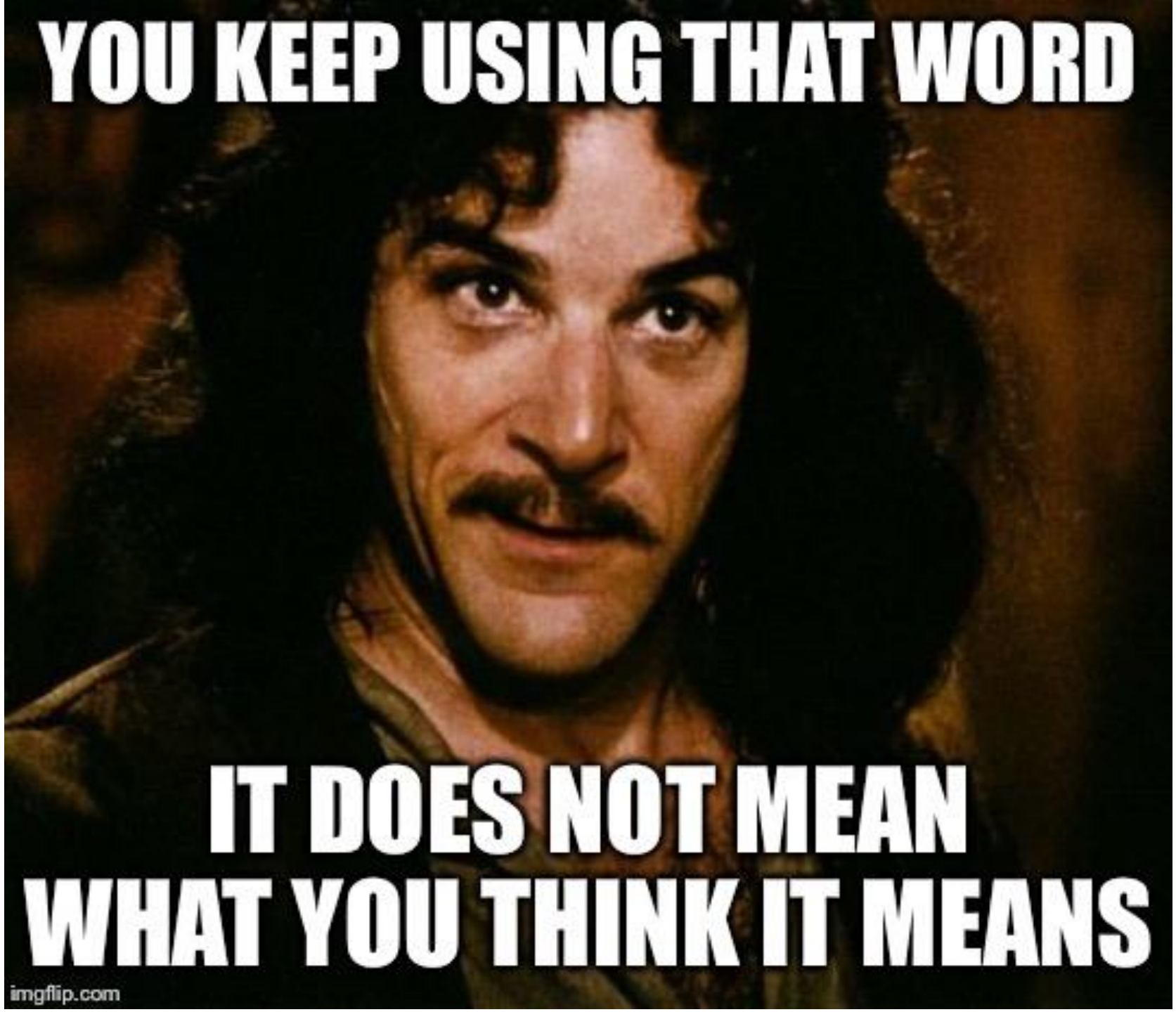
Die CEOs der Welt prognostizieren für 2024 wieder ein Wirtschaftswachstum. Nach wie vor gelten Cyberrisiken als grösste Bedrohung, wie eine Umfrage von PwC zeigt.

Januar 2024

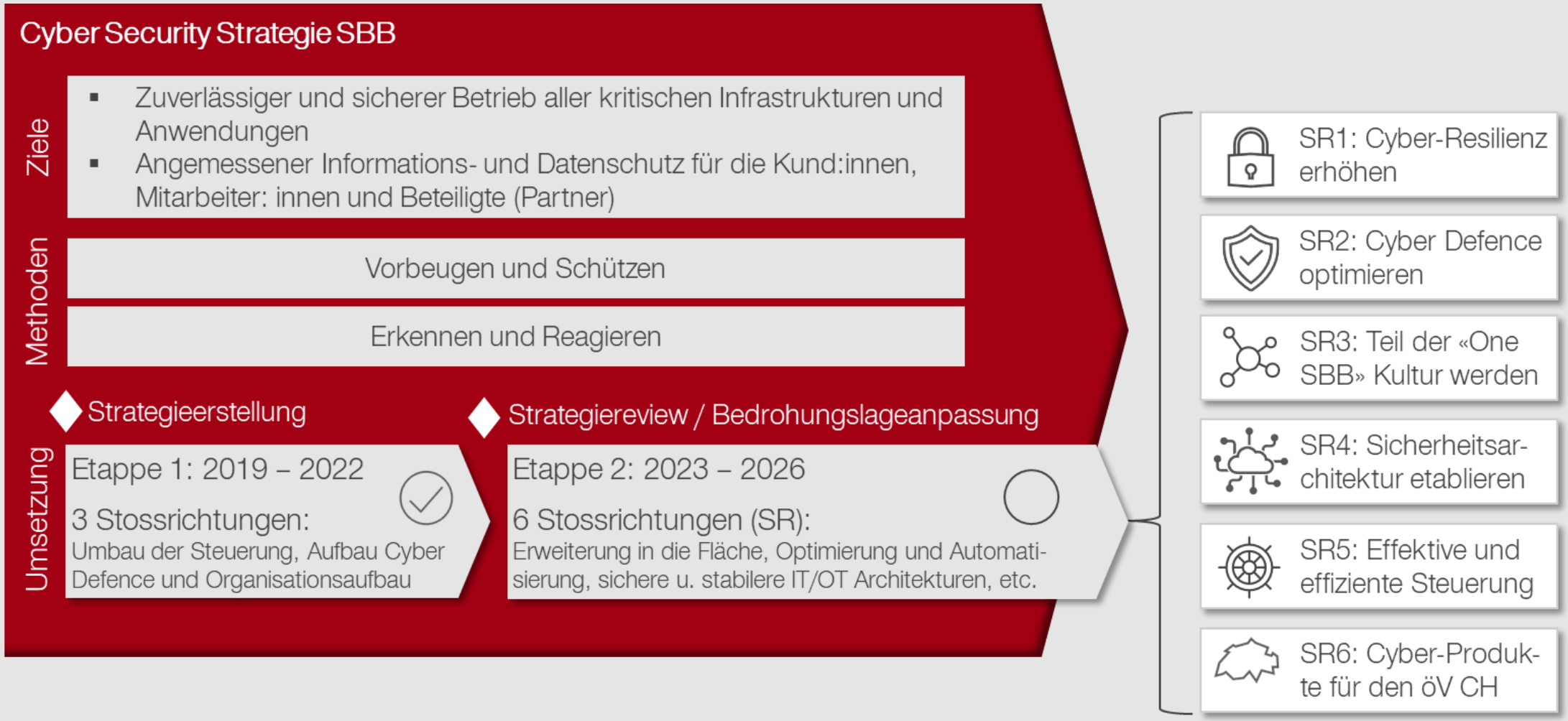
Quelle: Schweizer CEOs sehen Cyberrisiken 2024 als Topbedrohung | Netzwoche

September 2023

Quelle: Bundesamt für Raumentwicklung ARE auf LinkedIn: #sbb #cybersicherheit #mobilitätskonferenz #chmoko23


YOU KEEP USING THAT WORD
IT DOES NOT MEAN
WHAT YOU THINK IT MEANS
imgflip.com

Wohin wir gehen: Cyber Strategie 2026



Cyber Solution

Cyber Defence ART

ART Trio

- Rail ISAC (RUST)
- SOC Analysis (Flagship)
- Application Security (Unicorn)
- Advanced Cyber Defence (Octave)
- Vulnerability Management (Ruby)
- SOC Engineering (Darwin)
- System Team (Delphi)

cyberART

ART Trio

- Shared Service Architektur & Prozesse (Luna)
- Awareness (Action)
- Policy & Compliance (Go)
- InfoSec Assessments & Audits (Eagle)
- Datenschutz (Groovy)
- InfoSec Consulting (Fortran)

Was macht die Cyber Defence?

... ausser MEMEs im Internet suchen

... und sich dabei Malware einfangen.

Cyber Defence für Anfänger

Die CDC Value Streams.

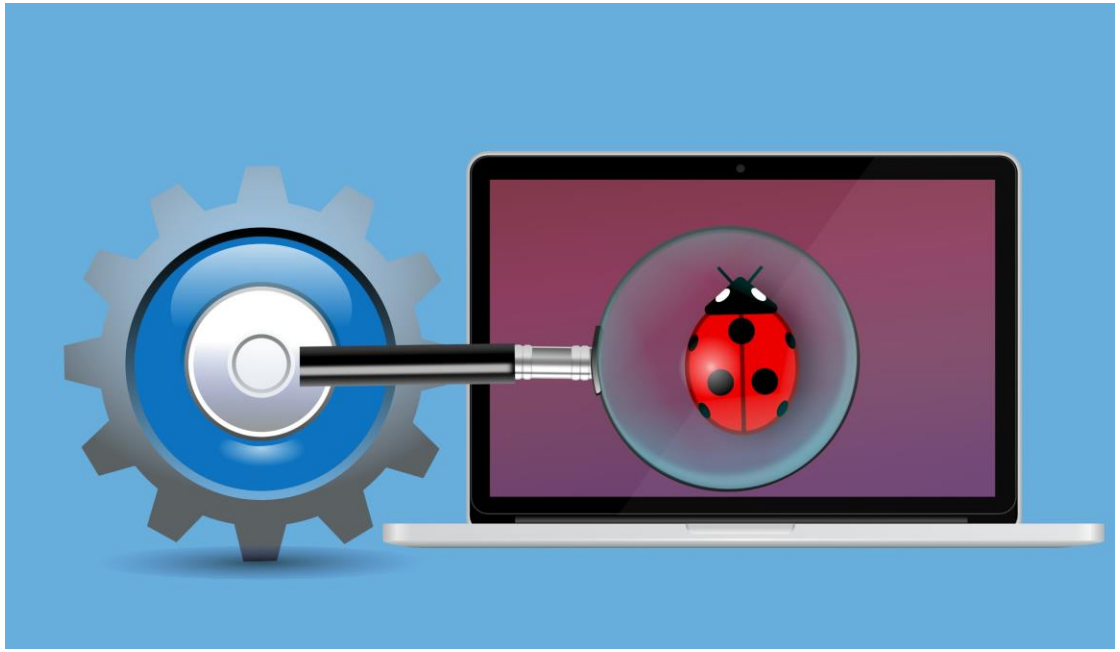
Cyber Angriffe	vorbeugen (best effort)
Cyber Angriffe	erkennen und reagieren (7x24)
Cyber Angriffe	unterstützende Services erbringen (Office hours, AdHoc)
Cyber Angriffe	Information Sharing and Analysis (Office hours, AdHoc)

Stuff Pick

Software Schwachstellen.

- Sind eine spezielle Art von Fehlern in einer Anwendung, welche von Angreifern ausgenutzt werden können
- Ziele:
  - Funktion der Anwendung stören
  - Daten stehlen
  - Daten verändern
  - … und damit Geld verdienen.

Schwachstellen Management.



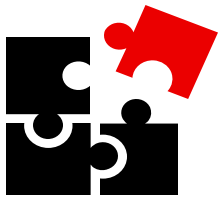
Wir liefern die Transparenz – Die Systembetreiber müssen sie verwalten.

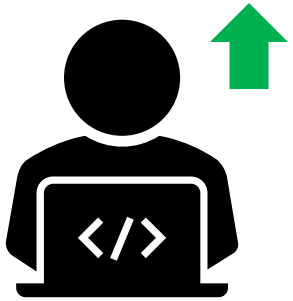
Warum?

- Die Risiken im Griff halten und mitigieren.
- Sensitive Daten schützen.
- Angriffen vorbeugen.
- Richtig reagieren.

Threat Modeling.

- Verbesserung der Kenntnisse über ein Produkt in den verschiedenen Rollen.
- Schulung des Sicherheitsbewusstseins im Team.
- Kontinuierliche Aufdeckung von Sicherheitsproblemen.





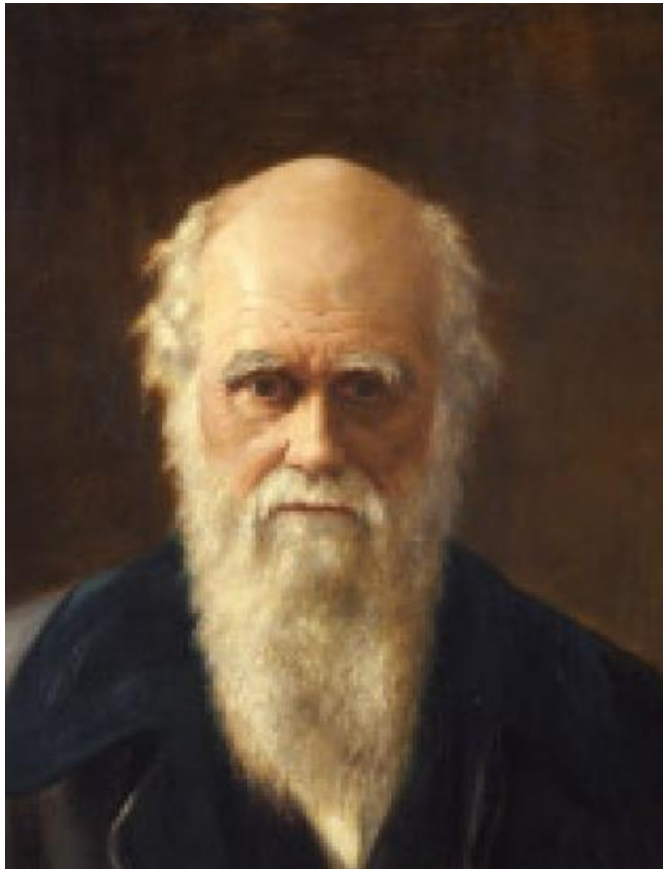
Threat Modeling im Detail.

Diagramm	Identifizieren	Mitigieren	Test
Was bauen wir?	Was kann schief gehen?	Was machen wir damit?	Sind unsere Massnahmen effektiv?

SOC – Security Operations Center – Team Flagship

- Gefahren frühzeitig erkennen, Angriffe detektieren und stoppen (7x24)
- Vorfälle bearbeiten
- Proaktives Security Monitoring (MS Defender, Audit Logs, Firewall Logs)
- Übungen mit anderen OEs und Betreibern

SOC Engineering – Team Darwin.



- Transparenz schaffen, Daten sammeln.
- UseCases definieren und implementieren.
- Testing.
- Automatisierung.

Beispiel UseCase 0146 - User added to high privilege group.

Angriffsvektoren und Risiken identifizieren	Logonboarding	UseCases definieren	UseCase implementieren und dokumentieren	UseCase testen	UseCase optimieren
– Wir machen risikobasierte Informationssicherheit – Viele Angriffsszenarien können von den Systembetreibern überwacht werden Im Beispiel hier: – Ein Angreifer kann einem Benutzer hohe Privilegien geben	– Datenquellen identifizieren und ins SIEM integrieren – Ereignisse und Indikatoren identifizieren Im Beispiel hier: – Quellsystem ist das SBB Anmeldungssystem MS AD und MS AAD – Das Ereignis ist, wenn ein Nutzer zu einer hoch Priviligierten Gruppe hinzugefügt wird	– Logik definieren, um die gewünschten Alarme zu erhalten. Im Beispiel hier: – Einen Alarm erzeugen wenn ein Nutzer zu einer hoch Privilegierten Gruppe hinzugefügt wird – Nutzer wird durch Analysten kontaktiert – Nutzer wird falls nötig gesperrt – Passwort reset	– Logik implementieren, um die gewünschten Alarme zu erhalten. – Dokumentation (Playbook) erstellen was der Analyst tun soll, wenn der Alarm auftritt	– Die Logik wird zuerst auf dem Test-System implentiert und getestet. – Allenfalls müssen noch Anpassungen gemacht werden, um in allen Fällen einen Alarm zu erhalten oder wenn unnötuge erzeugt werden. Im Beispiel hier: - Ein Nutzer wird einer Priviligierten Gruppe hinzugefügt - Gruppe dem UseCase hinzufügen	– Allenfalls werden trotz Tests zu viele oder zu wenige Alarme erzeugt Im Beispiel hier: - Kommunikation einrichten wenn das IAM Team Ein Nutzer wird einer Privilegierten Gruppe hinzufügt - Playbook automatisieren

CERT - Computer Emergency Response Team.

- Wird bei der SBB bei grösseren Vorfällen aktiviert.
- Das CERT-Team ist interdisziplinär aufgestellt.
- Es analysiert und bewertet die Bedrohung und leitet die nötigen Massnahmen ein

Wie arbeitet das CERT.

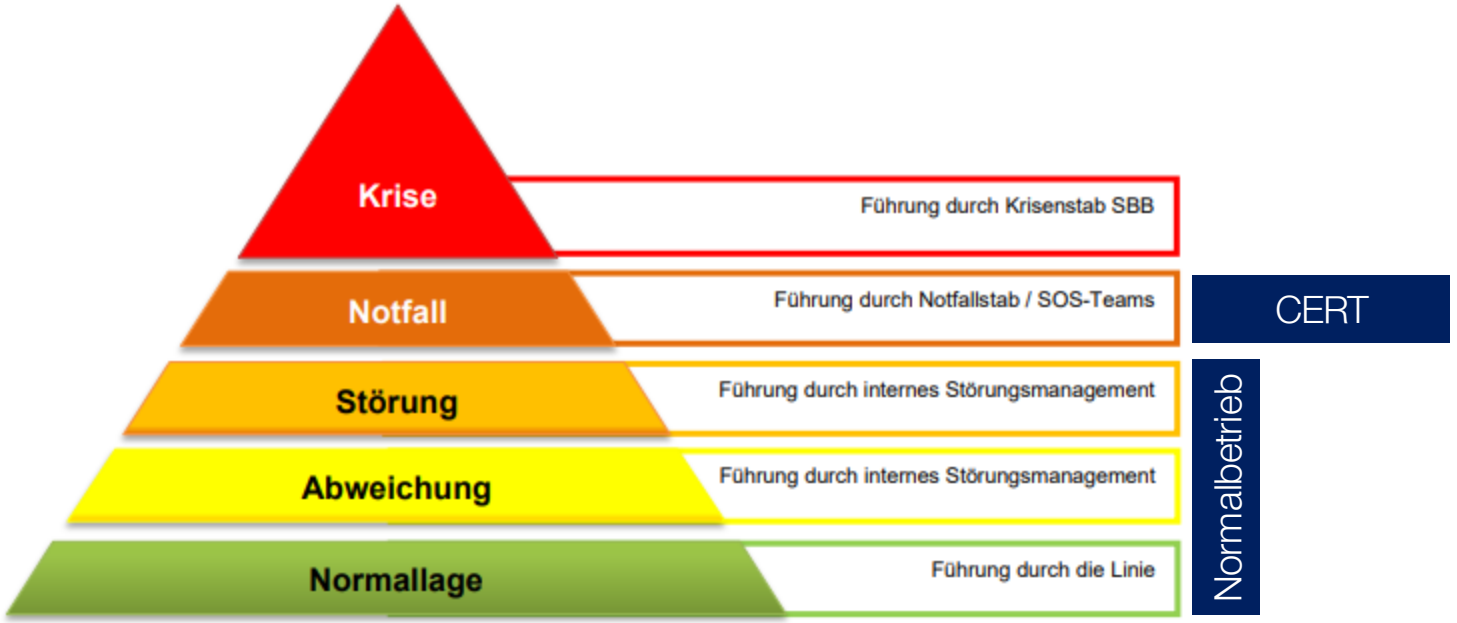
«Ad-hoc SBB CERT».

Regelwerk SBB | K 208.1 | SBB CFF FFS

Regelwerkversion	1-0	Vertraulichkeitsklassifikation	Intern
Gültig ab	1.11.2021	Eigner	SP-KRI
		Betroffene Prozesse	Notfall- und Krisenmanagement steuern
		Verfügbare Sprachen	DE, FR, IT
Betroffene Divisionen / Bereiche	Konzernbereiche, Infrastruktur, Produktion Personenverkehr, Markt Personenverkehr, Immobilien und Konzerngesellschaften		
Spezifische Empfänger / Verteiler	LIDI (elektronisch): A2, A20		
Ersatz für	I-B 80104		
Zuordnung	K 208.0		

Handbuch Notfall- und Krisenmanagement SBB

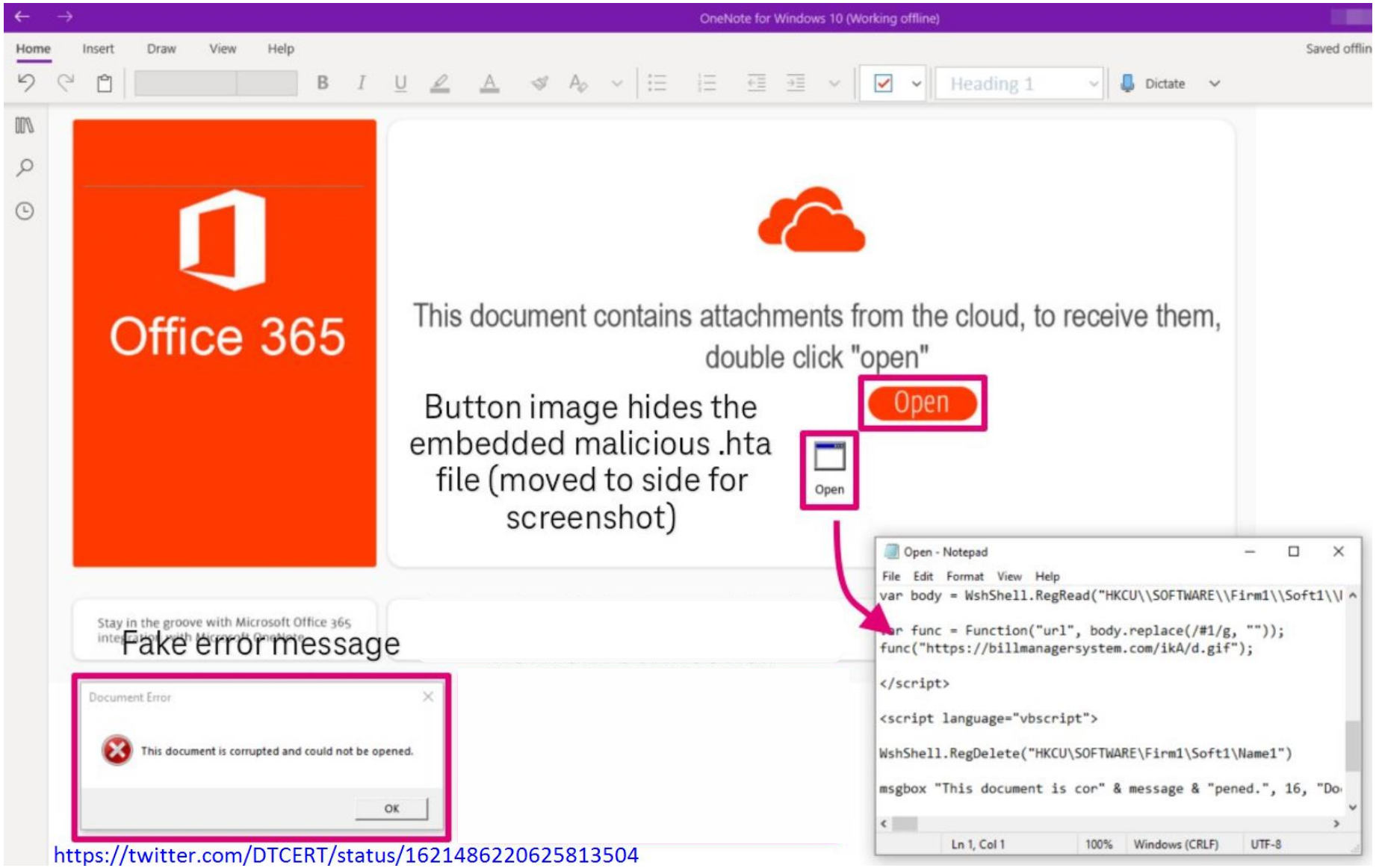
Zurück zum Normalzustand – so schnell wie möglich



Laut dem Handbuch Notfall- und Krisenmanagementhandbuch (K 208.1) ist das SBB CERT ein "SOS-Team" und für die Bewältigung von Cyber-Notfällen zuständig.

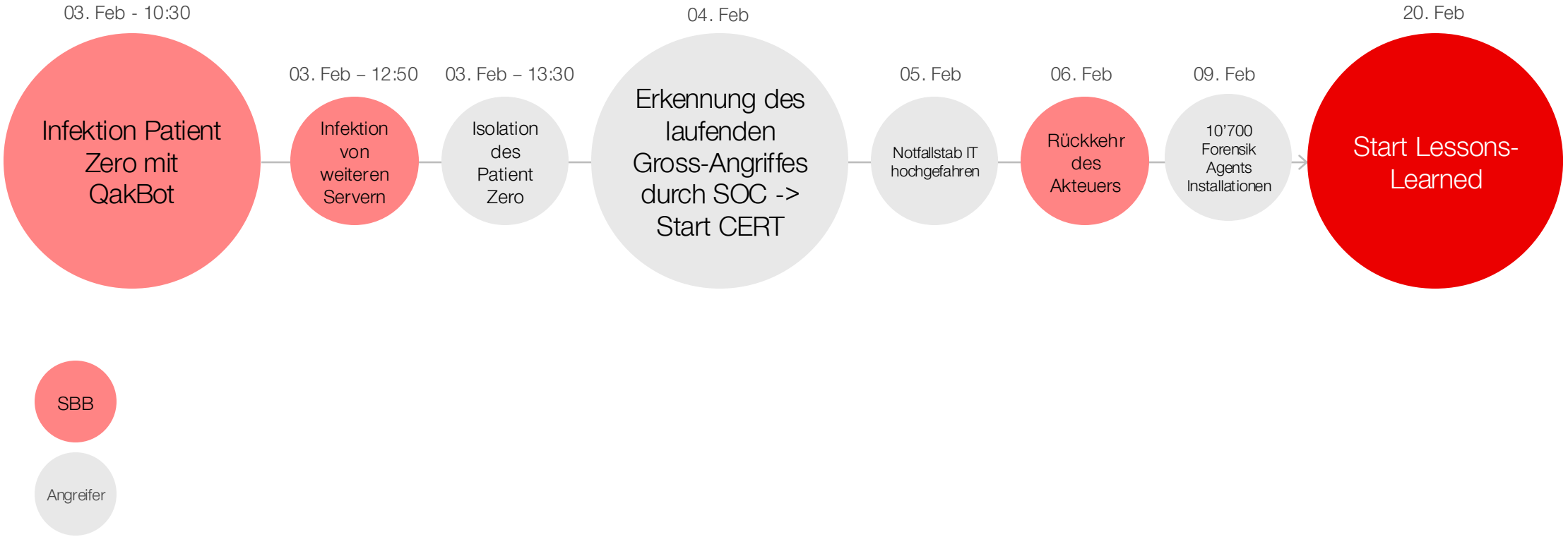
Es war einmal …

… ein unschuldiger Brief mit einem netten kleinen Geschenk beigefügt



https://twitter.com/DTCERT/status/1621486220625813504

CERT003 – Timeline.



Penetrationstest oder Ethical Hacking.

- Ziel eines Penetrationstests: Schwachstellen **proaktiv identifizieren.**
- Ein Penetrationstest wird klar strukturiert gemacht, um den Auftraggeber nachvollziehbar die Schwachstellen aufzuzeigen.
- Die Befunde werden bezüglich der Kritikalität beurteilt.

Bug Bounty bei der SBB.

- Die SBB ruft ethische Hacker auf, unsere Webseiten auf Schwachstellen zu prüfen. Dadurch sollen Datenabflüsse, insbesondere von Kundendaten, sowie Datenmanipulationen verhindert werden.

- Bug-Bounty-Programme sind ein beliebtes Instrument, um Sicherheitslücken in Softwaresystemen zu identifizieren und zu beheben. Finden die Teilnehmenden eine Bedrohung, winkt ihnen eine Belohnung.

- Schwachstellenidentifikation
- Früherkennung von Sicherheitslücken
- Verbessertes Sicherheitsbewusstsein
- Kostenersparnis

Source: Platform Leaderboard – Intigriti
Screenshot: 1.11.2023

CDC-Systeme – System Team Delphi.

Für die Erfüllung unserer Aufgaben benötigen wir verschiedene Werkzeuge und Plattformen:

- Eigene Hardware in einem isolierten Netz
- Schwachstellen Scanner
- MISP
- Asset Management
- Verschiedene Forensik und Tools

IT-Forensik.

- Wie die Forensik aus den Krimis nur auf IT-Mittel beschränkt.
- Analyse von:
  - Cybervorfällen
  - Compliance Verstössen

Rail ISAC MISP.

- MISP sammelt und speichert verschiedene Arten von Cyberbedrohungsinformationen
- Es dient dem Austausch von Bedrohungsinformationen zwischen verschiedenen Organisationen (Bahnen)

Support our Teams.

- Melde Vorfälle.
- Sei Wachsam bei Emails, Nachrichten auf das Handy, Anrufe.
- Lass dich nicht unter Druck setzen.
- Nutze einen zweiten Kanal, um dich zu versichern.
- Halte deine Applikationen aktuell.
- Dokumentiere deine Systeme
- Soziale Medien: Digitalen Fussabdruck prüfen, hinterfragen und reduzieren.

Nützliche Links.

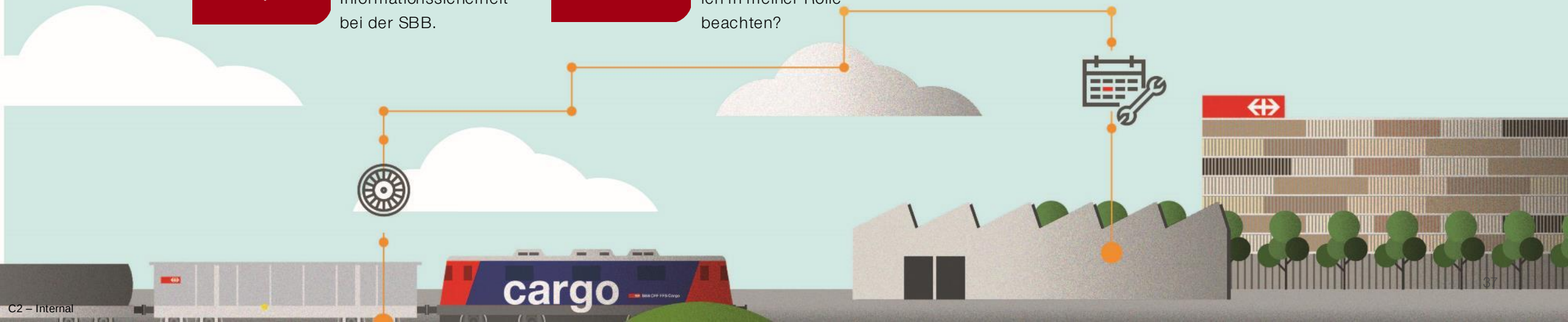
Anfrage über das cyberDesk
Ich will eine Beratung, Schulung oder einen Schwachstellenscan etc.

Über Cyber Solution
Mein Ausgangspunkt um mehr über den Cyber Solution zu erfahren.

Cyber-Vorfall melden
Verdächtiges melde ich an den ICT-Servicedesk
+41 51 220 30 40
ict.servicedesk@sbb.ch

InfoSec Communication Site
Mein Startpunkt für alles Wissenswerte über Informationssicherheit bei der SBB.

InfoSec und IT Vorgabenprotal
Gibt es dazu eine Weisung - was muss ich in meiner Rolle beachten?




SBB CFF FFS
Danke, merci
& grazie.

Konzernsicherheit.