

# **Arbeitsdossier - Systemsicherheit**

## **182 - Systemsicherheit implementieren**

## Systemsicherheit ist ein Prozess – keine ARBEIT!

Die Gewährleistung der Sicherheit innerhalb einer Infrastruktur bzw. eines datenverarbeitenden Systems darf nicht als Aufgabe bzw. Projekt betrachtet werden. Vielmehr handelt es sich hierbei um einen Prozess, welcher aktiv gelebt, unterhalten und vorangetrieben werden muss. Warum?

Die heutige Zeit punktet mit Innovationen, hoher Vernetzungsdichte, täglich neuen Technologien, Fluktuation von Mitarbeitenden, länderübergreifenden Kooperationen von Unternehmungen und/oder Privaten sowie Bevölkerungsschichten, bei welchen die monetären Motive klar überwiegen.

Das heisst für die Informatik-Branche, dass die zu realisierenden Massnahmen (um sich vor den dauernd wechselnden Gegebenheiten schützen zu können) ebenso eine hohe Kadenz an den Tag legen müssen. Aufgrund der hohen Umsetzungsgeschwindigkeit gilt es zudem die bereits implementierten Massnahmen zyklisch zu prüfen, sodass sichergestellt werden kann, dass bereits installierte Lösungen immer noch den aktuell gegebenen Bedrohungslagen Genüge tun.

## Diskussion zur Systemsicherheit

**Frage 1) Welche Systemsicherheitsmassnahmen mussten Sie bereits einmal implementieren, welche Sie heute als obsolet (überflüssig) betrachten können?**

.....

.....

.....

.....

.....

.....

**Frage 2) Wie sieht es bei Ihrem Arbeitgeber aus? Wird Systemsicherheit, aus Ihrer Sicht, als Prozess gelebt?**

.....

.....

.....

.....

.....

.....

**Frage 3) Was halten Sie heute von der Aussage "Never touch a running system"?**

.....

.....

.....

.....

.....

## Beispiel DRP

Bei der Sicherheitsdisziplin „Desaster Recovery Plan“ sollte es sich klassischerweise um ein ideales Beispiel handeln, welches die Sicherheit als Prozess betrachtet und nicht nur als einmalige Arbeit.

### Szenario 1

Sie wurden beauftragt „Acronis True Image“ zu implementieren. Nachdem Sie sämtliche Sicherungsjobs konfiguriert haben, führen Sie jeden Task einmal durch. Acronis finalisiert den Auftrag mit einem grünen Haken (alles OK). Sie melden Ihrer vorgesetzten Stelle, dass Ihr Auftrag erledigt ist.

### Szenario 2

Sie wurden beauftragt „Acronis True Image“ zu implementieren. Nachdem Sie sämtliche Sicherungsjobs konfiguriert haben, führen Sie jeden Task einmal durch. Acronis finalisiert den Auftrag mit einem grünen Haken (alles OK).

Anschliessend löschen Sie gewählte Systemverzeichnisse, welche Windows zum Beispiel für den Betrieb benötigt (z.B. System32), und versuchen die nicht mehr existenten Systembereiche wiederherzustellen. Zudem erstellen Sie eine Checkliste, welche diesen Test 3-6 Mal pro Jahr vorsieht. Sie melden Ihrer vorgesetzten Stelle, dass Ihr Auftrag erledigt ist.

**Frage 4) Für welches der beiden Szenarien entscheiden Sie sich? Begründen Sie bitte Ihre Antwort.**

.....

.....

.....

.....

.....

**Frage 5) Gesetzt der Fall, Sie arbeiten bei einem IT-Dienstleister... wie könnten Sie hier das von Ihnen gewählte Szenario am besten umsetzen?**

.....

.....

.....

.....

.....

.....

## Beispiel Firewall

Bei Ihrem Arbeitgeber wird sicherlich eine Firewall betrieben.

**Frage 6) Wie ist das Know-How innerhalb des IT-Teams verteilt? Wer kann und darf die Firewall aufgrund von welchen Vorschriften administrieren?**

.....

.....

.....

.....

.....

.....

**Frage 7) Wie könnten Sie sicherstellen, dass Sie (in der Rolle Firewall-Admin) von sämtlichen Änderungen (z.B. neue Serversystem werden von einem anderen IT-Team angeschafft und im LAN implementiert) erfahren auch wenn Sie nicht Bestandteil des Projektes waren?**

.....

.....

.....

.....

.....

.....

## Der Blick von aussen kann helfen... muss aber nicht!

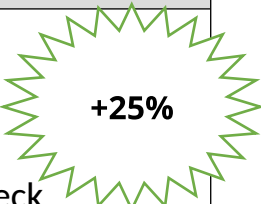
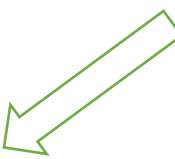
Wir sind uns vermutlich alle einig, dass wir uns nur vor dem schützen können, was uns bekannt ist.

Bevor wir uns jedoch auf diesem bereits recht hohen Level bewegen können, sind folgende Schritte im Vorfeld zwingend von Nöten:

- Aktuelle und vollständige Systemdokumentation
- Asset-Management ist lückenlos geführt/ vollständig (Inventur über HW und SW)
- Grundschutz wurde angewendet (Update, IDS/ IPS, Firewall, AV etc. → Härten)
- Erweiterter Grundschutz inkl. Risikoanalyse wurde auf exponiertes System angewendet

Wenn diese vier Grundpunkte realisiert sind, kann ein Blick von aussen auf unsere IT-Infrastruktur durchaus sinnvoll sein. Sprich, wir holen uns eine Drittmeinung... welche die sogenannte Betriebsblindheit zu brechen vermag.

Sie sollten auch hier jedoch vorsichtig sein. Zum einen sollte dieses Vorgehen mit dem Drittanbieter vertraglich geregelt werden. Zudem werden Sie auch hier nur weiter 25% gewinnen können... denn es gilt:

		Die Eigenschaften sind einem selbst ...	
		...bekannt	...unbekannt
Die Eigenschaften sind anderen...	...bekannt	<b>A</b> Öffentliche Person	<b>C</b> Blinder Fleck 
	...unbekannt	<b>B</b> Privatperson (mein Geheimnis)	<b>D</b> Unbekanntes 

**"D"** werden Sie **NIE** abdecken können. Weder als Privatperson noch als Unternehmung. Hier gilt der Grundsatz von "GMV" (Gesunder Menschenverstand). Oder in anderen Worten "Mut zur Lücke"!

Dritte, welche Ihre Infrastruktur aus technischer und organisatorischer Sicherheit testen, nennen sich Penetration-Tester. Sie versuchen während eines definierten Zeitfensters Ihre Unternehmung zu korrumpieren bzw. einen Weg in Ihre Infrastruktur zu finden. Seriöse Anbieter definieren Ihren Wirkungsraum mit Ihnen zusammen im Vorfeld und halten die Vereinbarung schriftlich fest.

# Die Vektoren der Systemsicherheit

Damit das Verständnis geschärft werden kann, sollten Sie die Systemsicherheit aus unterschiedlichen Blickwinkeln betrachten können. Analog dem ISO/OSI-Model in der Netzwerktechnik, bietet sich auch hier eine strukturierte Denkweise an.

Ein möglicher Ansatz kann die Aufteilung in unterschiedliche Disziplinen sein (dient als Idee und hat keinen Anspruch auf Vollständigkeit):

- **Raum/Gebäude**
  - Schliesssysteme/ Zutrittsregelung
  - Überwachung/ Kontrolle
  - Brandschutzvorkehrungen
  - Lüftung/ Klimatisierung
- **Hardware**
  - CPU
  - Speichertypen
  - Nicht zertifizierte Peripherie von Dritten
- **Netzwerk**
  - Zonenmodel/ VLANs
  - Adressräume
  - Perimeter-Firewall/ dedizierte Firewalls
- **Treiber**
- **Betriebssystem**
  - Grundinstallation und Grundkonfiguration
  - Netzwerktechnische Erreichbarkeit der OS-Instanz
  - Desktop-Firewall
  - Erweiterte Software und Drittdienste
  - Update-Verhalten
  - Zuständigkeiten/ Verantwortlichkeiten

Spätestens jetzt dürfte Ihnen klar werden, dass ein solches Sammelsurium nicht von einer einzelnen Person allein bewältigt werden kann. Hierfür ist die Arbeit im Team und abteilungsübergreifend Pflicht. Zudem benötigen Sie das Management, welches Ihnen das „Ausmass“ Ihrer Massnahmen bekannt gibt (zum Beispiel: *RPO darf nicht grösser als 12h sein; RTO darf nicht grösser als 18h sein*).

## Aufgabe/ Auftrag

Sie erstellen eine Präsentation, innerhalb einer 2er-Gruppe (Bei ungerader Anzahl ist eine 3er-Gruppe möglich). Ziel der Präsentation ist, dass Sie im Plenum einen Systemangriff vorstellen. Folgende Punkte werden dabei erwartet:

- Name des ausgewählten Angriffs
- Technische Erklärung des Angriffs (inklusive Fachbegriffe)
- Wie hoch ist die Wahrscheinlichkeit, dass der gewählte Angriff in Ihren Betrieben erfolgreich durchgeführt werden kann bzw. wie hoch ist das Risiko für Ihr Unternehmen?
- Welche Punkte von C.I.A. werden verletzt?
- Welche Schutzmassnahmen sind möglich?

Verfassen Sie zudem eine Textpassage, für die hausinterne ICT-Policy „*Umgang mit ICT-Infrastruktur auf Administrator-Level*“, welche dem organisatorischen Schutz (bezogen auf Ihren Angriff) nützlich sein kann.

## Zeit

- 50 Minuten für die Vorbereitung, 4 bis 6 Minuten für die Präsentation

## Erwartetes Ergebnis

- Eine sauber gestaltete Präsentation z.B. mit Google Presentation, Power Point, Flipchart usw.