Monti
Stampa
Furrer

Cyber Security für KMU

Frühschoppen der Zuger Treuhänder-Vereinigung ZTV

Zug, 26. Mai 2021

1 BEDROHUNG & ABWEHR

2 MENSCHEN

3 PROZESSE

4 TECHNIK

5 LEITFÄDEN & FRAGEBÖGEN

1 BEDROHUNG & ABWEHR

Rund ein Viertel aller KMU wurden bereits angegriffen. Auch Ihre Kronjuwelen sind für einige Angreifer-Gruppen von Interesse.

Cyber Akteure

Hacktivisten

- Eine Kombination von Hackern und Aktivisten. Diese Klasse von Angreifern verwendet ihre Hacker-Fähigkeiten, um eine potitisches Ziel zu verfolgen.
- Oft geht es um die Durchsetzung der Informationsfreiheit.

Beispiele von Akteuren

- Greenpeace

Vandalen, Hobby-Hacker

- Jemand, der sich etablierter und potenziell automatisierter Techniken aus dem Darknet bedient, um Systeme anzugreifen.
- Hohes Interesse daran, eine Jagdprämie mit hohem Wert präsentieren zu können.

- Studenten

Staatliche Akteure

- Gehört einer staatlichen Organisation an und führt offensive Angriffe mit dem Zweck der Spionage oder Sabotage aus.
- Oder von einer staatlichen Organisation vorgeschobene Angreifer..

- Nord-Korea
- China
- Russia
- USA

Cyber-Kriminelle

- Cyber-Kriminelle greifen Systeme aus finaziellem Interesse an.
- Diese Angreifer haben ein sehr hohes Know-How und sind bestens organisiert.
- Sie nutzen bekannt werdende Schwachstellen sofort aus.

- Mafia (Italien)
- Mafia (Russia)
- Triades (China)

Terroristen

- sind politisch motivierte Angreifer, die Informations- und Kommunikations-Technologie einsetzen und diese angreifen, um mit schweren Zerstörungen Angst und Schrecken zu verbreiten.

- IS/Daesh

Insider

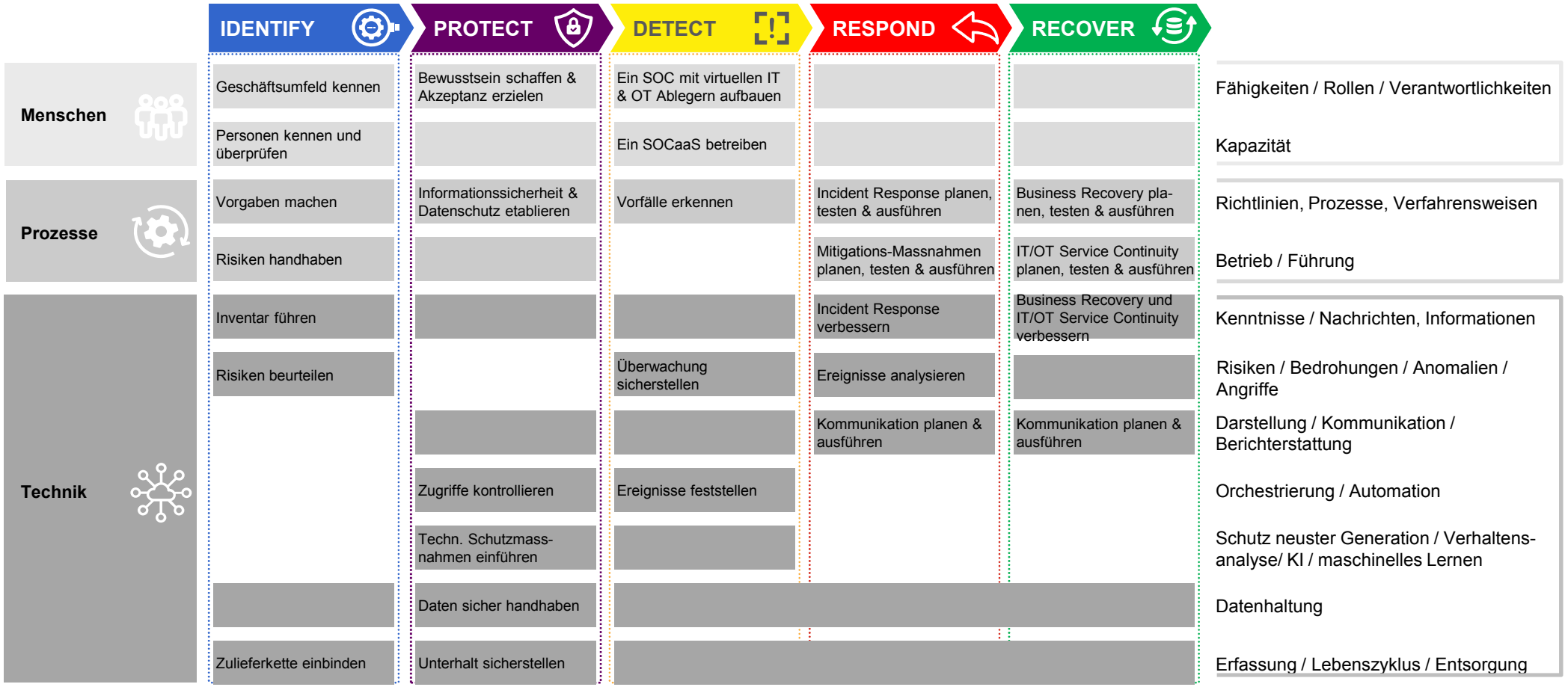
- Die Position und die Rollen eines Mitarbeitenden und damit verbundene Systemprivilegien sind eng mit den möglichen anrichtbaren Schäden verknüpft.
- Dies gilt auch für Systeme, die angeblich völlig sioliert sind.

- Aktuelle und frühere Mitarbeitende oder Externe

Nicht jede Gruppe von Cyber-Akteuren greift mit derselben Motivation an.
Es geht darum, zu verstehen **wer, warum** und **mit welcher Wahrscheinlichkeit** angreifen will.

Für grössere Firmen hat sich das NIST Cybersecurity Framework = der IKT-Minimalstandard des BWL etabliert.

Cyber Abwehr



Für kleinere Firmen empfehle ich den Cybersecurity-Leitfaden für KMU[1].

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

ICTSWITZERLAND ISSS Information Security Society Switzerland satw it's all about technology SNV SQS ASA | SVV

[1] https://ictswitzerland.ch/content/uploads/2020/03/Leitfaden_Cybersecurity_Schnelltest_D.pdf

2 MENSCHEN

Machen Sie alle Mitarbeitenden und Partner von VR & GL bis zu Assistenz und Hauswart für die Sicherheit in ihrem Bereich verantwortlich und sensibilisieren Sie sie fortlaufend.

- ☐ Regeln Sie die **Verantwortung** der Mitarbeitenden aller Stufen.
- ☐ Bezeichnen Sie einen **Beauftragten für die Cybersicherheit** und unterstellen Sie diesen direkt der GL.
- ☐ Lassen Sie die **Revisioren** beurteilen, ob die Vorkehrungen für Cybersicherheit & Datenschutz genügen.

- ☐ Verankern Sie die **Sensibilisierung** Ihrer Mitarbeitenden im Unternehmensalltag.
- ☐ Sorgen Sie mit starken **Passwörtern** und **MFA** für den bestmöglichen Schutz Ihrer Systeme und Anwendungen.
- ☐ Definieren Sie **Benutzerrichtlinien** für einen sicheren Umgang mit Geräten, Internet und E-Mails.

- ☐ Fordern Sie von **Lieferanten und Drittbetreibern** über die gesamte Lebensdauer die Umsetzung derselben Cybersecurity-Massnahmen vertraglich ein, die Sie selber anwenden.
- ☐ Achten Sie beim Auslagern von **IT-Security-Dienstleistungen** auf Zertifikate und die Einhaltung der nach Ihren Risiken gebotenen Sicherheitsmassnahmen.

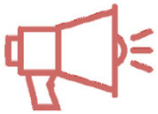
Trotz aller Technik sind es die Mitarbeitenden, welche für die Sicherheit Ihres Unternehmens entscheidend sind. Dazu ist es nötig, dass Sie und alle Mitarbeitenden die aktuellen Gefahren kennen, mit den technischen Mitteln umgehen können sowie die minimalen Regeln einhalten.

3 PROZESSE

Richten Sie Ihre Organisation auf die Bedrohungen und Risiken aus und definieren Sie die entsprechenden Prozesse.

- ☐ Sichern Sie Ihre Informationen mit einem regelmässigen **Backup** auf ein unabhängiges Medium.
- ☐ Sorgen Sie für eine externe **Aufbewahrung** das Backup an einem geschützten und vom Netzwerk getrennten Ort.
- ☐ Überprüfen Sie regelmässig, ob sich die Daten von den Sicherheitsmedien zurückspielen lassen (**Restore**).

- ☐ Sorgen Sie für eine geeignete **Benutzeradministration**. Lassen Sie getrennte Konten für Adminaufgaben (besonders schützenswerte Daten, Informationen und Systeme) und «normale» Aufgaben einrichten.
- ☐ Verwenden Sie nur persönliche Konten (keine Konten verwenden, die von mehreren Benutzerinnen und Benutzern mit gleichem Benutzernamen/Kennwort verwendet werden).
- ☐ Vergeben Sie die **Zugriffsrechte rollenbasiert** (z.B. Buchhaltung/Personaladmin/Sekretariat/Verkauf)
- ☐ **Sperren** Sie **bei Austritten** und Übertritten die Konten/Rollen der entsprechenden Personen.



- ☐ Erstellen Sie einen **Notfallplan**: Identifizieren Sie kritische Systeme, halten Sie fest, wer damit arbeitet, definieren Sie Rückfallebenen (Ersatz-PCs, zwei Browser; Vereinbarung über Reaktionszeiten und Lieferfristen mit Lieferanten).
- ☐ Definieren Sie die erste **Reaktion** bei einem Vorfall: Definieren Sie u.a., wer bei einem Vorfall (z.B. bei einer Lösegeldforderung) zu informieren ist.
- ☐ Erstellen Sie einen Entschärfungsplan (**Mitigation**): Trennen Sie z.B. die Netzwerkverbindungen (LAN-Kabel, WLAN) der betroffenen Systeme.
- ☐ Definieren Sie Massnahmen zur schnellen Wiederherstellung (**Recovery**) Ihrer Systeme.
- ☐ Üben Sie den Notfall in Ihrem Unternehmen.

Bei einem Cyber-Vorfall sind Vorbereitung und Reaktion zentral und entscheiden darüber, ob und wie schnell Sie Ihr Business nach einem Vorfall weiter betreiben können. Eine rasche und richtige Reaktion kann Schäden entscheidend verringern oder sogar vermeiden.

4 TECHNIK

Nutzen Sie die Möglichkeiten moderner Technik. Beziehen Sie die ICT als betreute Commodity (Microsoft 365, Google Workspace) aus der Cloud

- ☐ Nutzen Sie moderne **Hard- und Software** (z.B. Firewall, Endpoint Protection Platform/Endpoint Detection & Reaction mit AI/ML, früher Antiviren-Software), um Ihre Sicherheit zu erhöhen.

- ☐ Achten Sie auf eine **regelmässige Aktualisierung** Ihrer Software (Betriebssystem, Office-Software, Browsers, übrige Applikationen und Utility Programme).
- ☐ Verbinden Sie **veraltete Geräte**, bei denen kein Softwareupdate verfügbar ist, nicht mit dem Internet oder – noch besser – ersetzen Sie sie.

Durch Sicherheitslücken können Unbefugte in Ihre Systeme eindringen. Software Updates schliessen diese Sicherheitslücken. Eine aktuelle Firewall und eine moderne Endpoint Protection kann Ihre Computer schützen.

- ☐ Machen Sie Sie den **Datenschutz** zum integralen Bestandteil der Cyber Security.
- ☐ Schützen Sie **schützenswerte / besonders schützenswerte Daten** von Personen (z.B. Kunden oder Mitarbeitende), die Sie auf irgendeine Art und Weise bearbeiten[1], nach DGS/DSGVO hinreichend.
- ☐ Überbinden Sie diese Schutzverpflichtung vertraglich im Detail allfälligen für Sie an dieser Verarbeitung beteiligten Dritten (**Auftragsverarbeitung**).

Ihr Unternehmen ist verantwortlich für den sicheren Umgang mit Personendaten und geistigem Eigentum. Cybersicherheit und Datenschutz gehen Hand in Hand: Durch einen Cyberangriff können Kriminelle an sensible Daten gelangen.

[1] insb. das Beschaffen, Erfassen, Übermitteln, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten.

5 LEITFÄDEN & FRAGEBÖGEN

Orientieren Sie sich an einem für Ihre Firmengrösse geeigneten Leitfaden und beurteilen Sie Ihren Reifegrad jährlich mit Hilfe eines Fragebogens.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

ICTSWITZERLAND ISSS Information Security Society Switzerland satw it's all about technology SNV SQS ASA | SVV

- ☐ Cybersecurity-Leitfaden für KMU
- ☐ Cybersecurity-Schnelltest für KMU (Kurzversion)
- ☐ Cybersecurity-Schnelltest für KMU (Langversion)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Nationales Zentrum für Cybersicherheit
NCSC

- ☐ Merkblatt Informationssicherheit für KMU

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für wirtschaftliche Landesversorgung BWL

- ☐ IKT-Minimalstandard
- ☐ IKT-Minimalstandard – Assessment Tool

DSAT

Datenschutz Self Assessment Tool

- ☐ Datenschutz-Self-Assessment-Tool: Inhaltsübersicht, Anleitung und Glossar (V6.01)

Monti
Stampa
Furrer

Besten Dank für Ihre Aufmerksamkeit

Für weitere Fragen stehe ich Ihnen gerne zur Verfügung.

ivo.maritz@msfpartners.com, www.msfpartners.com