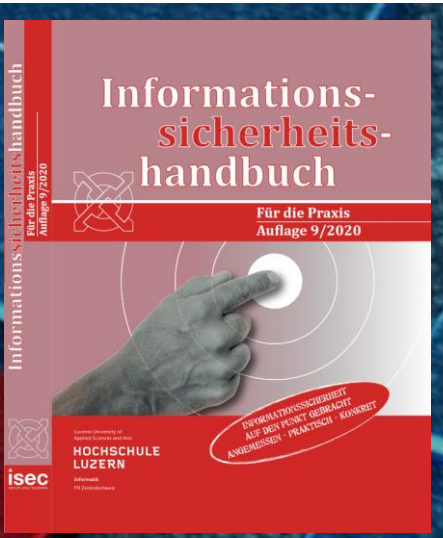
Cyber-Security für Unternehmer & Private

SIDLER Information Security

FabLab Zug - Wissen & Essen – 6. Dezember 2022

Cyber-Angriff und Verteidigung

FAB LAB ZUG



Mitautor
IT-Sicherheitshandbuch für die Praxis
ISBN: 3-9521208-3-9 www.sihb.ch

Wolfgang Sidler
Inhaber SIDLER Information Security GmbH
Datenschutz- (DPO) und Security-Officer (CISO)
www.sidler-security.ch

Gib Phishing-Mails keine Chance!
So entlarvst Du Cyberkriminelle

Phishing-E-Mails ähneln Nachrichten von Eurer Bank, Arbeitskollegen, Lieferanten, Freunden oder sogar von Deinem Chef. Auch wenn sie vertrauenswürdig aussehen, enthalten sie oft Hinweise, die ihre wahren oder bösartigen Absichten verraten.

Wenn Du eine E-Mail erhältst, die mehrere der folgenden Phishing-Indikatoren enthält oder sich einfach **nicht «richtig» anfühlt, wende Dich umgehend an unseren IT-Help Desk** – bevor noch mehr Leute betroffen sind...

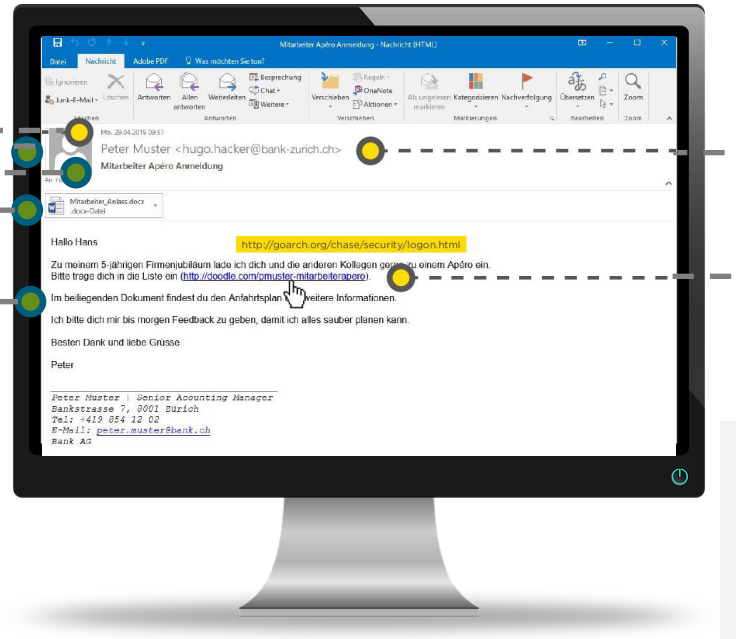
Datum
Wurde die E-Mail zu einer ungewöhnlichen Uhrzeit geschickt (Nacht, Wochenende)?

Empfänger
- Wurde die E-Mail noch an andere Personen geschickt?
- Falls ja: Kennst Du diese Personen?
- Sind es ungewöhnlich viele?

Betreff
Stimmt der Betreff mit dem Inhalt überein?
- Ist es eine Antwort auf eine E-Mail, die Du geschickt oder angefordert hast?
- Ist der Betreff persönlich oder eher allgemein formuliert?

Anhang
Erwartest Du eine entsprechende Datei?
Falls der Absender von intern stammt:
- Stimmt der Dateiname mit den bei Deinen üblichen Bezeichnungen überein?
- Wirkt der Dateiname vertrauenswürdig?
- Ist es ein üblicher Dateityp?
- Hat der Virenscanner die Datei gemeldet?
- Beinhaltet das Dokument Makros? (Nicht aktivieren!)

Inhalt
- Ist die Ansprache unpersönlich?
- Wird eine Aktion von Dir verlangt (Herausgabe/Eingabe Logindaten, Zahlungsaufforderung etc.)?
- Wird mit Konsequenzen gedroht, beispielsweise bei Nichtreaktion (Geldverlust, Strafanzeige, Konto- oder Kartensperrung etc.)?
- Hat der Text Rechtschreib-/Grammatikfehler oder eine unübliche Formatierung?
- Sieht die Signatur/der Footer vertrauenswürdig aus?
- Werden verschiedene Schriftgrössen, -formatierungen, -farben etc. verwendet?



Absender
- Kennst Du den Absender?
- Falls ja: Ist es dieselbe E-Mail-Adresse wie beim letzten E-Mail-Kontakt?
- Wurde die E-Mail von einem Bekannten, Partner oder Lieferanten geschickt, ist inhaltlich aber ungewöhnlich resp. uncharakteristisch?
- Stimmt die E-Mail-Adresse mit dem Anzeigenamen des Absenders überein? (Peter Muster → hugo.hacker@bank-zurich.ch)
- Handelt es sich bei der E-Mail-Adresse um eine gefälschte Domain? (@bank-zurich.ch → @bank.ch)

Hyperlinks
Wenn Du mit der Maus über den Link fährst (s. links in gelb):
- Wird dieselbe Zieladresse angezeigt? (Achtung: Auf keinen Fall klicken!)
- Ist der Link ungewöhnlich lang?
- Wird im Text Bezug zum Link genommen?
- Ist die Zieladresse des Hyperlinks fehlerfrei? (z.B. www.apple.com → www.appple.com)

Allgemeine Tipps
Höre auf Dein Bauchgefühl: Wenn Du nicht sicher bist, ob die E-Mail echt oder ein Betrug ist, lass die E-Mail lieber durch unseren IT-Help Desk überprüfen.

Klicke bei Unsicherheiten niemals auf einen Link und öffne auf keinen Fall die Datei.

Wenn Du vermeintlich sichere Anhänge öffnest und eine Warnmeldung erscheint, lass die E-Mail durch unseren IT-Help Desk überprüfen.

Im Zweifelsfall in einer neuen, separaten E-Mail oder telefonisch beim Absender nachfragen, ob er/sie tatsächlich diese E-Mail geschickt hat.

ONE STEP AHEAD

SIDLER Information Security

ÜBER 10 JAHRE FÜR SIE DA

In Bezug auf Ransomware Attacken ist eine stufengerechte Sensibilisierung aller Mitarbeitenden sehr wichtig.

Sie sollen die Fähigkeit entwickeln Phishing-Mails erkennen zu können.

FAB LAB ZUG

Ransomware 10-Punkte-Check

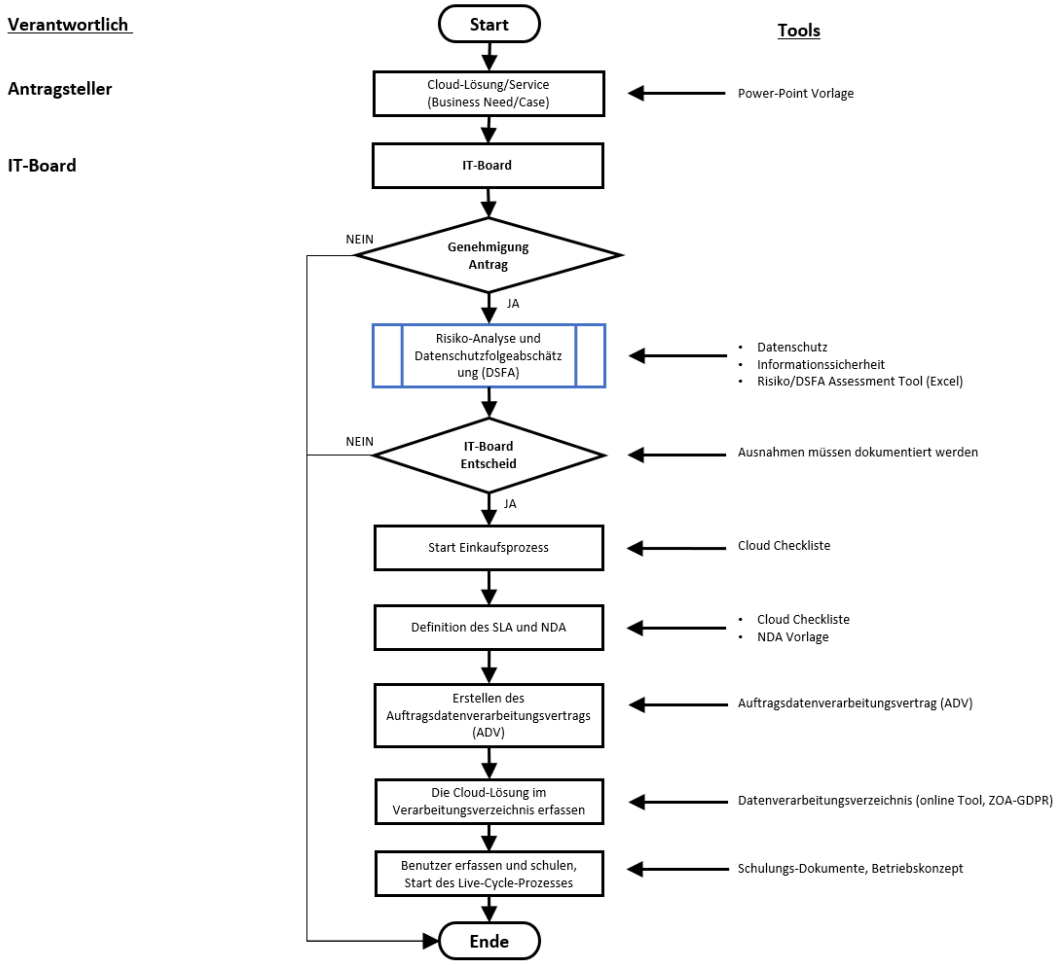
1. Wiederherstellbarkeit der geschäftskritischen Prozesse innert nützlicher Frist
2. Backup-Infrastruktur gemäss dem 3-2-1 Prinzip
   - Drei Kopien aller wichtigen Daten, zwei verschiedene Speichertypen, mindestens ein Backup offline/unveränderlich
3. Vorbereitung für den Ernstfall (Krisenmanagement) → Notfall- und Krisenmanagement Handbuch
4. Durchgängige Sicherheit bei allen Schnittstellen ins Unternehmensnetzwerk
   - Klar definierte VPN-Zugänge, 2FA, externer Scan der vom Internet aus erreichbaren Server & Services
5. Sichere Konfiguration der Endgeräte
   - OS aktuell halten, XDR-Client, Patch-Management, GPOs ausrollen, keine Admin-Rechte, etc.
6. Absichern der Administrator Zugriffe
   - Möglichst wenige Admin-Accounts, persönliche Admin-Accounts, 2FA
7. Eingeschränkte Zugriffsberechtigungen (RBAC)
   - Benutzer-Berechtigungskonzept für die Anwendungen, On/Off-Boarding Prozess, need-to-know Prinzip
8. Netzwerksegmentierung
   - Das Office-Netzwerk vom Produktions(OT)-Netzwerk mit Firewalls trennen
9. Patch-Management
   - Alle Systeme, Server und Endgeräte mit den neuen Versionen aktualisieren. Gilt auch für die Anwendungen wie PDF-Reader, etc.
10. Unterstützung durch einen externen Partner innert 24h (SOC)
    - Sorgen Sie dafür, dass Sie im Ernstfall innert nützlicher Frist kompetente Unterstützung erhalten.

Was ist der Nutzen einer wirksamen Informationssicherheit?

- Geringere Verwundbarkeit
- Keine falsche Sicherheit
- Bewussterer Umgang mit Information
- Gefahren kennen, Restrisiko kennen
- Sorgfaltspflicht erfüllt (IKS)
- Besseres Image nach Aussen
- Positive Audits (interne und externe Revision)
- Erhöhtes Kundenvertrauen mit einer ISO 27001 Zertifizierung
- Einhalten aller Gesetze (IKS, Datenschutz, GebüV, FINMA, MDR/IVDR, Pharma, etc.)
- Wettbewerbsvorteil und Kundenbindung → Sicherheit schafft Vertrauen
- Reduziert das Risiko einer Geschäftsunterbrechung erheblich (hohe Verfügbarkeit)
- Fördert das „Sicherheitsbewusstsein“ aller Mitarbeitenden (Sicherheitskultur)
- Steigert die Möglichkeit neue Geschäfts-Felder sicher und schneller anzugehen
- **Ist der Schlüssel für eine erfolgreiche Digitalisierung**

Hier die Lösung für einen sicheren Cloud-Einsatz

- Erstellen einer Cloud-Weisung mit Prozess
- Etablieren eines IT-Board Gremium, um alle Anwendungen (on-prem und Cloud) zu prüfen und zu genehmigen
- Durchführen einer Cloud-Risiko Einschätzung
- Durchführen einer Datenschutzfolgeabschätzung (DSFA)
- Etablierung eines Lieferanten-Management-Prozess und Zertifizierungen z.B. ISO 27001.
- US Cloud Act Prüfung gemäss David Rosenthal
- https://www.rosenthal.ch/downloads/Rosenthal_Cloud_Lawful_Access_Risk_Assessment.xlsx



Sichere Einführung einer Cloud-Lösung

Risiko-Einschätzung einer neuen Cloud-Service:

- Wo werden die Daten physisch gespeichert?
- Wer hat Zugriff auf diese Daten?
- Entspricht die Cloud-Lösung dem Datenschutz und/oder GDPR?
- Wurde eine Datenschutzfolgeabschätzung (DSFA) durchgeführt?
- Wurde ein Auftragsdatenverarbeitungsvertrag (ADV) mit dem Cloud-Anbieter erstellt?
- Wie sieht es mit US Cloud-Act aus, wenn das Unternehmen Sitz in den USA hat?
- Verletzen wir durch diese Daten-Auslagerung eine bestehenden Kunden-Vereinbarung/Vertrag?
- Hat der Cloud-Provider eine ISO-27001 Zertifizierung?
- Ist ein Vertrag mit möglichen Ausstiegs-Szenarien vorhanden?
- Ist ein NDA vorhanden?
- etc.

6 Schritte für eine wirksame Sicherheit

Prävention ist besser als Reaktion !

1
- Sensibilisierung aller Mitarbeitenden
- Security Newsletter
- Fingierte Phishing Attacke
- E-Learning System mit Schulungsnachweis

2
- Risiko-Management auf GL-Ebene
- jährliche Risiko-Einschätzung z.B. mit IKS
- Top 5 Risiken bearbeiten
- Massnahmen priorisieren und umsetzen
- Wirksamkeit der Massnahmen prüfen

3
- Alle Server und Clients systematisch aktualisieren
- Patch-Prozess überwachen (KPI)

4
- Alle vom Internet erreichbaren Websites wie WebShop, VPN-Portal, etc. regelmässig auf Schwachstellen prüfen lassen

5
- SOC-Anbindung und alle IP-Geräte im Netzwerk regelmässig auf Schwachstellen prüfen lassen.

6
- Mit State-of-the-Art Cyber-Security Massnahmen einen IT-Grundschutz etablieren und aufrechterhalten.

Tipps (1/2) – nicht abschliessend …

- Verantwortlichkeiten in Sachen Cyber-Security und Datenschutz regeln
- Cyber-Security- und Datenschutz-Richtlinien/Weisungen erstellen, schulen und umsetzen

  Sonst hören Sie bei einem Vorfall: Das wurde mir nie gesagt …. Das wusste ich nicht …
- Backups erstellen und testen, ein Offsite (offline) –Backup einrichten
- Alle vom Internet erreichbaren IP-Adressen (Services) auf Schwachstellen täglich überwachen lassen (Vulnerability Service mit Alarmierung) – *meineimpfungen.ch war ein schlechtes Beispiel*
- Einsatz von Cloud-Lösungen/Services genau klären (Cloud-Policy)
- Wo immer möglich 2-Faktor Authentisierung einführen
- Alle Mitarbeitenden auf allen Stufen zielgerecht sensibilisieren
- Für den Notfall vorsorgen (Notfall- und Krisenmanagement-Konzept)
- IT-Systeme und Netzwerke regelmässig auf Schwachstellen überprüfen lassen
- Benutzerberechtigungen jedes Jahr prüfen (Lehrling hat meistens mehr Rechte als der CEO!) Ein- und Austritts-Checkliste erstellen.
- Wichtig ist, dass Sie Ihre Lieferanten kennen. Speziell jene mit einer online-Anbindung für Fernsupport.
- Führen Sie eine Risiko-Analyse durch und definieren Sie die Massnahmen zur Minderung der Risiken

Tipps (2/2) – nicht abschliessend …

SIDLER Information Security

- Wenn Sie IT-Dienstleistungen auslagern, achten Sie darauf, dass der IT-Dienstleister ISO-27001 zertifiziert ist.
- Verwenden Sie Office 365 aus der Cloud, dann bitte nur mit einer 2-Faktor Authentifizierung. Username mit Passwort reichen heute nicht mehr – Phishing Falle !
- Verschlüsseln Sie die Festplatten Ihrer Notebooks. Das gibt auch den Benutzer die Sicherheit bei einem Verlust des Notebooks.
- Halten Sie Ihre Programme immer aktuell (Patch-Management) !
- Setzen Sie unterwegs beim Notebook immer eine Sichtschutzfolie ein !
- Bei der Digitalisierung in Ihrem Unternehmen die Informationssicherheit und den Datenschutz nicht vergessen.
- Bei einer «komischen» Geld-Transaktion (Phishing E-Mail) immer telefonisch rückfragen und sich über die Transaktion informieren.
- Achten Sie darauf, dass es in Ihrem Unternehmen keine Schatten-IT gibt (wild installierte WLAN-Access Points, nicht sichere private Geräte am Unternehmens-Netzwerk, etc.)
- Verwenden Sie immer **«starke»** Passwörter – min. **12 Zeichen** und mit Sonderzeichen, noch besser MFA/2FA (2 Faktoren Authentisierung)
- Ändern Sie bei allen IT-Geräten immer das Default-Passwort, speziell bei IOT-Geräten
- Achten Sie darauf, dass in Ihrem Unternehmen vertrauliche Dokumente **«sicher»** vernichtet werden (Shredder oder Dokumenten-Vernichtungs-Service wie Reisswolf)

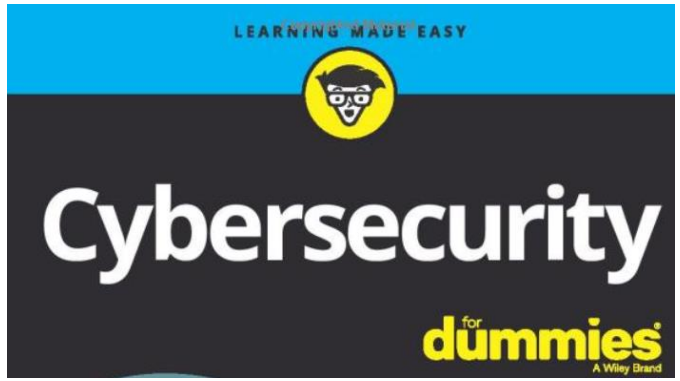
FAB LAB ZUG

Tipps für eine effektive Informationssicherheit

- Nominieren Sie intern eine Verantwortliche Person für die Informationssicherheit (CISO) oder mit einem externen Mandat – Security Officer as a Service
- Erstellen Sie ein Basis-Paket an internen Weisungen für den sicheren Umgang mit den Daten, der IT, Klassifikation von Informationen, Home-Office, Umgang mit social Media, etc.
- Etablieren Sie in Ihrem Unternehmen eine **«Sicherheits-Kultur»,** welche gelebt wird.
- Erstellen Sie einen Mitarbeiter ON/OFF-Boarding Prozesse und geben Sie den Mitarbeitenden und Externen nur die Benutzerrechte, welche sie für ihre Arbeit benötigen (RBAC). Nach dem Motto: Need-to-Know
- Verhindern Sie eine Schatten-IT, indem Sie die IT-Anforderungen Ihrer Stakeholder aktiv einfordern, transparent kommunizieren, sie über die Risiken aufklären und einen entsprechenden Bewilligungs-Prozesse für die Einführung von neuen Anwendungen on-premise oder in der Cloud.
- Etablieren Sie ein IT-Board (Gremium) mit Mitgliedern aus der Geschäftsleitung, CISO, DPO, Legal & Compliance, HR, Marketing/Kommunikation, etc., welches sich alle 2 Monate trifft und Entscheidungen fällt.
- Sensibilisieren Sie Ihre Mitarbeitenden **«stetig»** auf allen Stufen in Sachen Informationssicherheit und Datenschutz, um die **«Sicherheitskultur»** zu fördern.
- Sichern Sie Ihre IT mit den heute am Markt verfügbaren Security-Lösungen unter Einbezug auch von Managed Security Services (SOC).

Eine Bitte an die Benutzer …

- Diskutieren Sie geschäftliche Angelegenheiten **nicht** in der Öffentlichkeit oder mit Ihrer Familie!
- Teilen Sie keine Geschäfts-internen oder vertraulichen Informationen über WhatsApp, Facebook, Twitter und andere Social Media Kanäle !
- Bitte sperren Sie Ihren Computerbildschirm mit **«Ctrl-Alt-Del»,** wenn Sie Ihren PC/Notebook verlassen!
- Bitte befolgen Sie die **"Clear-Desk"-**Richtlinie und halten Sie Ihren Schreibtisch frei von vertraulichen Informationen
- Lassen Sie nicht zu, dass andere Ihre geschäftlichen Gespräche mithören (in Restaurants, öffentlichen Verkehrsmitteln, usw.) !
- Versenden Sie keine **«privaten»** E-Mails mit dem Geschäfts-E-Mail Account !
- Vernichten Sie **«interne & vertrauliche»** Dokumente mit dem Schredder oder benutzen Sie die speziellen Reisswolf Alu-Behälter.
- Lassen Sie sich nicht täuschen ! (Social Engineering, Phishing eMail)



Links

www.kmuschutz.ch

www.ncsc.admin.ch

www.mobiliar.ch/versicherungen-und-vorsorge/angebote-fuer-unternehmen/ratgeber/it-und-datensicherheit-wichtige-regeln-fuer-mitarbeitende

https://cybero.ch/cyber-security-check

https://haveibeenpwned.com

https://www.sidler-security.ch/de/cyber-security-check