Informationssicherheit und Datenschutz

SIDLER Information Security

SWISS BUSINESS PROTECTION

BNO-Informationsabend – 6. November 2019 in Sarnen

Cyberkriminalität und Datenmissbrauch – eine Bedrohung für jedes Unternehmen!

Wolfgang Sidler
Inhaber SIDLER Information Security Gmbh
VR & Founding Partner Swiss Business Protection AG
Datenschutz und Security-Officer
www.sidler-security.ch

Wolfgang Sidler
Senior Security Consultant & CEO

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

- Master of Advanced Studies HSLU in **Information Security** und Certificate of Advanced Studies HSLU in **Blockchain**
- **20 Jahre** Informationssicherheits-Erfahrung
- **10 Jahre** Stv. Datenschutzbeauftragter des Kantons Luzern von 2009 - 2018
- **6 Jahre** IT-Security Officer bei der Privatbank Julius Bär in Zürich und New York
- **3 Jahre** internationale Security-Beratung (USA und Oman)

Kontakt
www.sidler-security.ch
wolfgang.sidler@sidler-security.ch

SWISS BUSINESS PROTECTION

Wirtschaftsschutz-Schweiz
Member of the Board & Founding Partner
Swiss Business Protection AG
www.swissbp.ch

Aktuelle Vorfälle

Cyberangriff legt Zürcher Firma lahm

Attacken auf IT-Systeme nehmen zu. Nun hat es die Firma Meier Tobler aus Schwerzenbach erwischt.

Verwaltungsratspräsident Silvan G.-R. Meier spricht an einer Medienkonferenz von Meier Tobler. (Foto: Keystone/Alexandra Wey)

Corsin Zander
Redaktor Zürich
@corsinzander

27.07.2019

Beim Schweizer Gebäudetechnik-Unternehmen Meier Tobler geht seit Mittwoch nichts mehr. Cyberkriminelle hatten in der Nacht die gesamte IT-Infrastruktur lahmgelegt. Dies berichtete gestern die TV-Sendung «SRF Börse». Auf ihrer Website wies Meier Tobler Kunden auf den Ausfall hin. Betroffen seien neben der Festnetz-Telefonie und allen E-Mail-Adressen auch das zentrale SAP-System sowie das Lagerleitsystem.


meier tobler

Cyberangriff auf Meier Tobler

Liebe Kunden

In der Nacht von Dienstag auf Mittwoch wurde die IT-Infrastruktur von Meier Tobler durch einen Cyberangriff lahmgelegt. Das zentrale SAP-System, das Lagerleitsystem, die Festnetz-Telefonie, die Website und alle E-Mail-Adressen funktionieren nicht.

Da Lager und Lieferlogistik direkt betroffen sind, können wir erst ab Anfang nächster Woche wieder Auslieferungen vornehmen.

Die Notfallpläne von Meier Tobler greifen. Alle unsere Marchés sind normal geöffnet und lieferbereit.

Unser e-Shop ist unter eshop.meiertobler.ch in Betrieb, Bestellungen können erfasst werden aber die Auslieferungen können erst ab Anfang nächster Woche erfolgen. Ihre direkten Ansprechpartner sind über die Ihnen bekannten Mobil-Nummern erreichbar und unterstützen Sie gerne.

Die Firma informiert die Besucher ihrer Website über die Cyberattacke. Screenshot: meiertobler.ch

Quelle: Tages Anzeiger 27.7.2019

Cyberangriff auf Meier Tobler

Liebe Kunden

In der Nacht von Dienstag auf Mittwoch wurde die IT-Infrastruktur von Meier Tobler durch einen Cyberangriff lahmgelegt. Das zentrale SAP-System, das Lagerleitsystem, die Festnetz-Telefonie, die Website und alle E-Mail-Adressen funktionieren nicht.

Da Lager und Lieferlogistik direkt betroffen sind, können wir erst ab Anfang nächster Woche wieder Auslieferungen vornehmen.

Die Notfallpläne von Meier Tobler greifen. Alle unsere Marchés sind normal geöffnet und lieferbereit.

Unser e-Shop ist unter eshop.meiertobler.ch in Betrieb, Bestellungen können erfasst werden aber die Auslieferungen können erst ab Anfang nächster Woche erfolgen. Ihre direkten Ansprechpartner sind über die Ihnen bekannten Mobil-Nummern erreichbar und unterstützen Sie gerne.

Aktuelle Vorfälle

Konsequenzen/Schaden:

negativ
- Ausfall der gesamten IT- und Telefonie-Infrastruktur für 4 Tage (5 Mio. Umsatzausfall)
- Image Schaden unbekannt
- Hohe Wiederherstellungskosten (ca. 1 Mio. CHF)

positiv
- Notfall- und Krisenmanagement-Plan waren vorhanden
- Proaktive Kommunikation mit Presse und Kunden

Fazit und Tipps
- Über einen guten IT-Grundschutz verfügen
- Notfall- und Krisenmanagement-Plan (BCM) bereit haben
- Datensicherung (Backup) Offsite (extern) haben
- Interne Weisung mit dem Umgang der IT-Mittel erstellen
- Alle Mitarbeitenden auf allen Stufen regelmässig zum Thema Sicherheit sensibilisieren
- Cyber Versicherung für den finanziellen Schaden abschliessen

Aktuelle Vorfälle

Auto AG fährt Systeme nach Hackerattacke

Letzte Woche ist die Rothenburger Auto AG von Hackern angegriffen worden. Ein Einzelfall w

Bei der Auto AG Group kehrt langsam wieder Normalität ein. Der Rothenburger Nutzfahrzeughändler ist vergangene

bar», sagt Auto-AG-CEO Marc Ziegler. Alle Daten seien wieder hergestellt worden und das Sicherheitsdispositiv habe man

Angriffe mit Verschlüsselungstrojanern auf Schweizer KMU gegeben hat.

Franken. Meier Tobler räumte ein, dass man von den Tätern erpresst worden sei. Den geforderten Millionenbetrag habe man

«Mittlerw
alle Systeme
alle Prozesse
in vollem Um

Auto AG Group

27. August 2019 18:24; *Akt: 27.08.2019 18:24*

Hacker attackieren Bus- und Truck-Betrieb

Hacker haben einen Geschäftsbereich der Auto AG Rothenburg lahmgelegt. Der Busbetrieb ist zwar nicht betroffen, aber der Handel mit Lastwagen. Eine Forderung ist noch nicht eingetroffen.

LUZERN

Medienmitteilung der Luzerner Polizei

Luzern, 27. August 2019

Hackerangriff auf die Auto AG Group

Rothenburg

Die Auto AG Group mit Sitz in Rothenburg wurde Opfer eines Hackerangriffs. Die Täterschaft ist unbekannt. Die Fahrgäste des öffentlichen Verkehrs sind vom Hackerangriff nicht betroffen.

Die Auto AG Group wurde Opfer eines Hackerangriffs. Die Täterschaft ist unbekannt. Wie gross der entstandene Schaden für die Auto AG Group ist bzw.

CEO / Vorsitzender der Geschäftsleitung
Auto AG Group
Stationsstrasse 88
6023 Rothenburg / LU
+41 79 604 30 74 Mobile

Kontakt
LUZERNER POLIZEI
Christian Bertschi
Chef Kommunikation
Kasimir-Pfyffer-Strasse 26
6002 Luzern
Tel + 41 41 248 80 11
E-Mail info.polizei@lu.ch

Impressum | Disclaimer

Luzerner Polizei | polizei.lu.ch

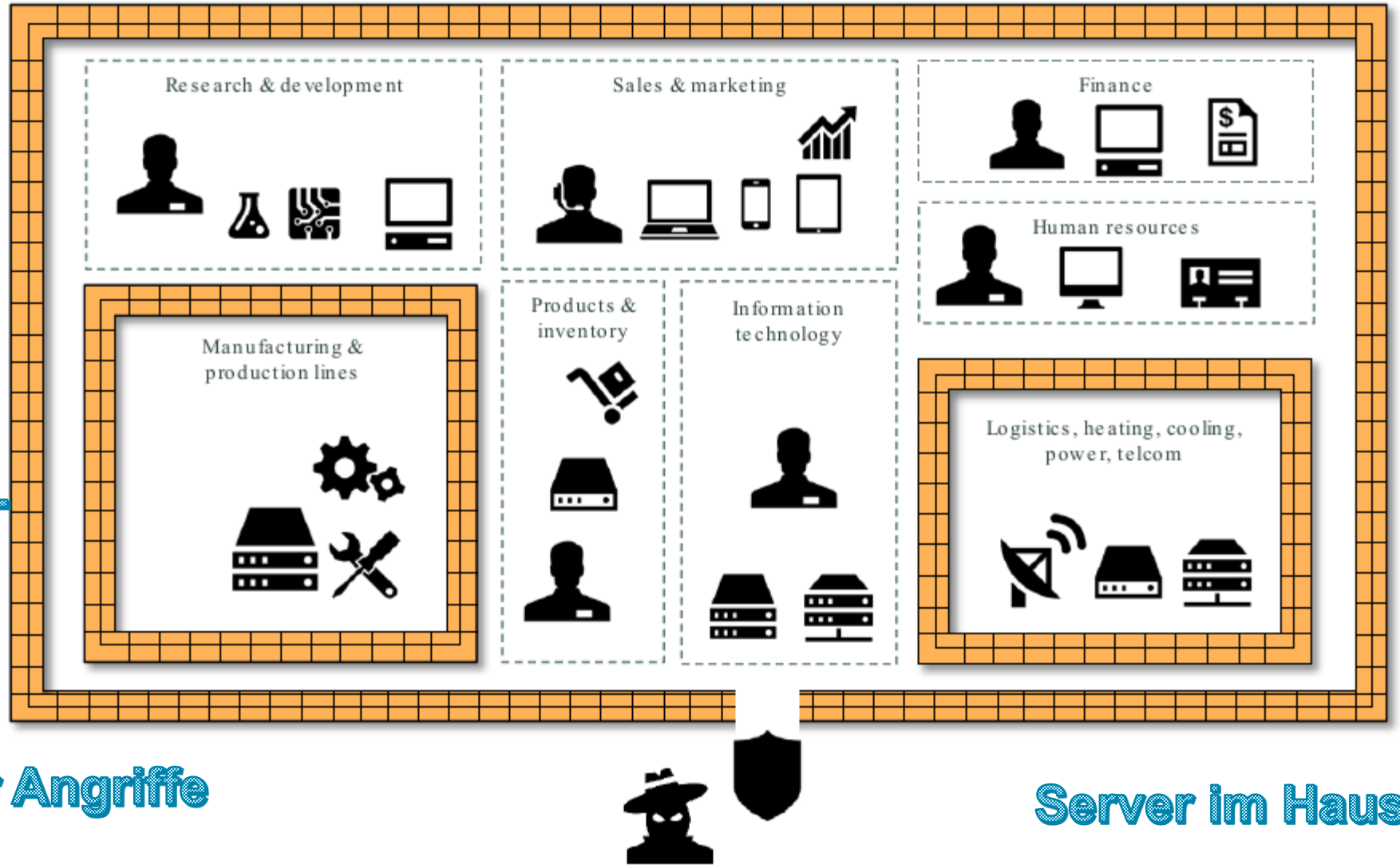
Also Hacker-Angriffe auf KMUs sind keine Fiction, sondern Realität!

Quelle:

Die “alte” IT-Business Welt

weniger Abhängigkeiten

keine Cloud Lösungen



Einen Internet-Anschluss

weniger Angriffe

Server im Hause

Die “neue” IT-Business Welt

Neue Schwachstellen

Neue Cloud-Lösungen

viele vertragliche Verpflichtungen

Neue Gesetze (DSGVO)

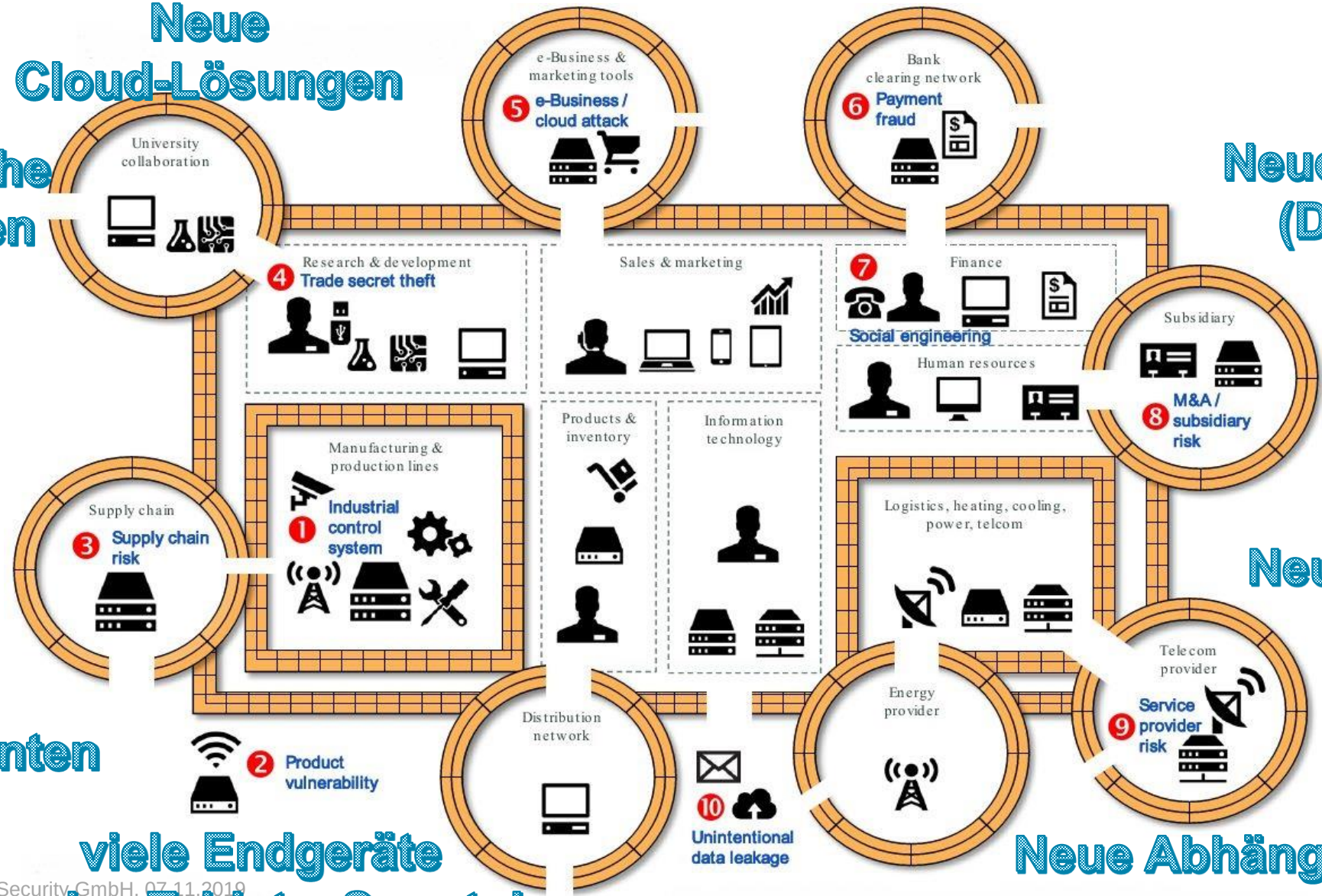
Neue Technologien wie IoT

Neue Angriffe

viele Lieferanten

viele Endgeräte Notebooks, Tablets, Smartphones

Neue Abhängigkeiten



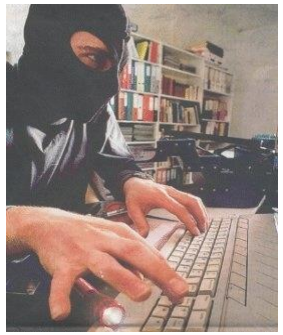
Allgemeine Gefahren und Risiken

Höhere Gewalt
Feuer, Blitz, Sturm, Überschwemmung, Stromausfall, Krankheit, …

Menschliches Versagen
Bedienungsfehler, Unwissen, falsches Verhalten, …

Gesetzliche Mängel
Nicht Einhalten der Gesetze, Reglemente etc. (Compliance)

Technisches Versagen
Netzwerkausfall, Software-Fehler, Viren, Disk-Ausfall, …



Organisatorische Mängel
Fehlende oder nicht angewendete Weisungen, unzureichende Zutrittskontrollen, falsche Zugriffsrechte, Abgang von Schlüsselpersonen (Know-how-Verlust), Versagen der Prozesse, …

Vorsätzliche Handlungen
Manipulation, Diebstahl, Missbrauch, Sabotage, Spionage, Hacking, Erpressung, Viren, organisierte Kriminalität, ...

Konsequenzen/Schaden:
- Produktions-Ausfall, Auslieferungs-Verzug, …
- Verlust von vertraulichen Daten oder Know-how
- Bussen (juristische Konsequenzen)
- Verstoss gegen vertragliche Geheimhaltungsvorschriften
- Image Schaden
- Wiederherstellungskosten

Top-Risiken aus einer Umfrage von 2017

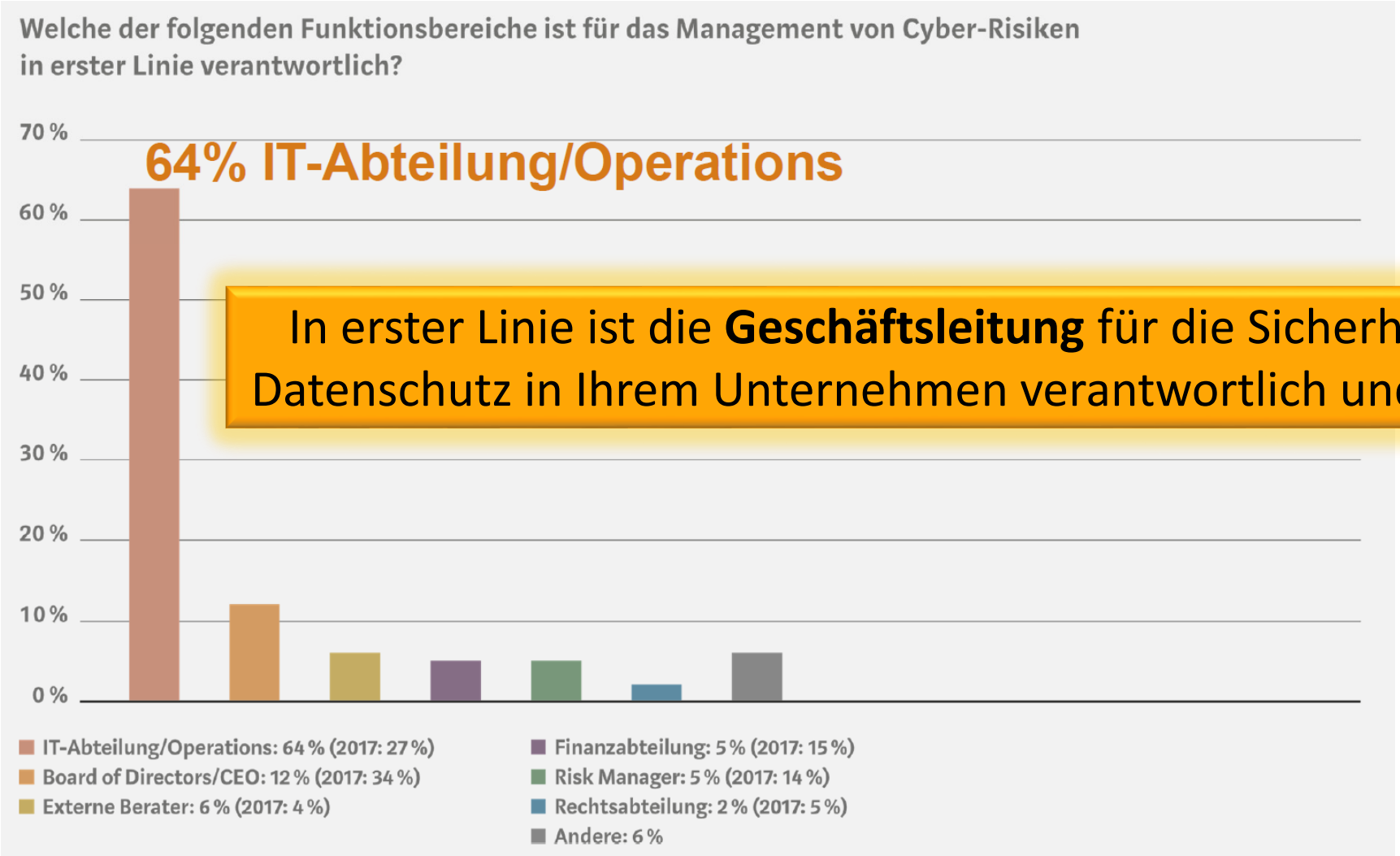
Die folgenden Top-Risiken wurden aktuell in Deutschland in einer aufwendigen Studie identifiziert. Über **20 Prozent** aller Unternehmen hatten in den letzten **drei Jahren** einen **konkreten Spionagevorfall oder einen Cyberangriff**.

Konkrete Handlung - Risiken	In %
Bewusste Informations- oder Datenweitergabe. Datendiebstahl durch eigene Mitarbeitende	**47.8**
Abfluss von Daten durch externe Dritte wie Zulieferer, Dienstleister oder Berater	**46.8**
Hackerangriffe auf die IT-Systeme und Geräte (Server, Notebook, Tablet, Smartphone)	**42.4**
Diebstahl von IT-Geräten (Notebook, Tablet, Handy)	**32.7**
Social Engineering (geschicktes Ausfragen von Mitarbeitenden) → Phishing, Tendenz steigend!!!	**22.7**
Sonstiger Informationsabfluss ausserhalb der Firma durch unbedachte Kommunikation, Home-Office, Cloud-Dienste wie Dropbox, etc.	**15.5**
Abhören und Mitlesen von elektronischer Kommunikation wie unverschlüsselte E-Mails	**12.2**
Einbruch in Gebäuden bzw. Diebstahl von Dokumenten, Unterlagen, etc.	**11.2**
Abhören von Besprechungen, Telefonaten, Mitlesen von Faxen oder Ausdrucke	**6.5**

50%

Studie: 6’924 Unternehmen in Deutschland wurden im Auftrag von TÜV befragt. 10.9% der Befragten Unternehmen waren Banken, Finanzdienstleistungen und Versicherungen.

Sicherheit ist “Chefsache”



In erster Linie ist die **Geschäftsleitung** für die Sicherheit und den Datenschutz in Ihrem Unternehmen verantwortlich und nicht die IT!

Menschliches Fehlverhalten

190,000 mobile phones left in London Taxis every year

Press Association

PUBLISHED
06/10/2014 | 09:02

SHARE

More than 190,000 mobile phones are lost in the back of London taxis each year, in what a security firm has called a technology "black hole". PA photo.

More than 190,000 mobile phones are lost in the back of London taxis each year, in what a security firm has called a technology "black hole".

In Zürich wurden in einem halben Jahr 3'250 Handys und 200 Laptops im städtischen Fundbüro abgegeben.

Tipp:

Verschlüsseln Sie die Festplatten Ihrer Notebooks und erstellen Sie eine Weisung für den «Umgang mit mobilen Geräten».

Fundsachen 07. Januar 2014 08:06; *Akt: 07.01.2014 10:19*

Pendler haben 12'000 Handys im Zug vergessen

100'000 Gegenstände haben Schweizer 2013 in Zügen und Bahnhöfen liegen lassen – vom Rollstuhl über Sexspielzeug bis zur Urne. Nur wenig mehr als die Hälfte davon holten sie ab.

1|2 Ein Metalldetektor, eine Urne, ein Rollstuhl und eine Beinprothese: Roland Widmer von Fundsachenverkauf.ch mit einigen der Fundgegenstände aus dem Jahr 2013.

Bild: hal

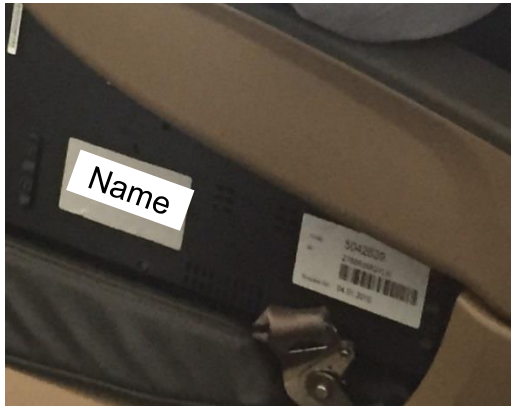
ein aus i

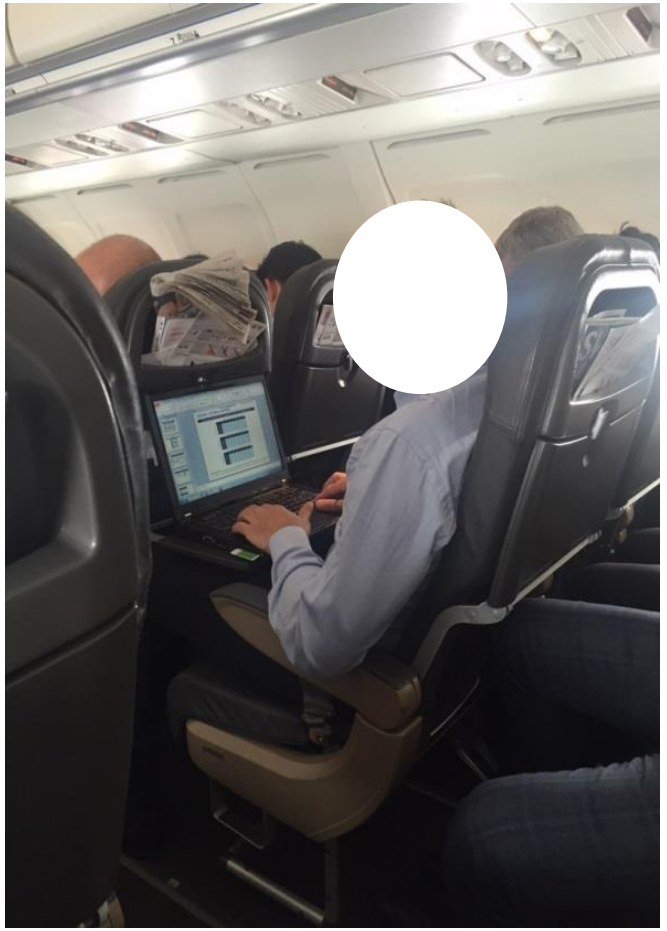
Taschen, Koffer, Kleider und Elektrogeräte: Im Keller des Fundsachenverkauf.ch in Zürich stapelt sich die Ware auf Holzpaletten und in Kisten mit Aufschriften wie «Spielzeug», «Schmuck», «iPhone» oder «Erotik». Hier landet, was in der Schweiz in Zügen und Postautos sowie an Bahnhöfen und Flughäfen liegen geblieben ist und nicht abgeholt wurde.

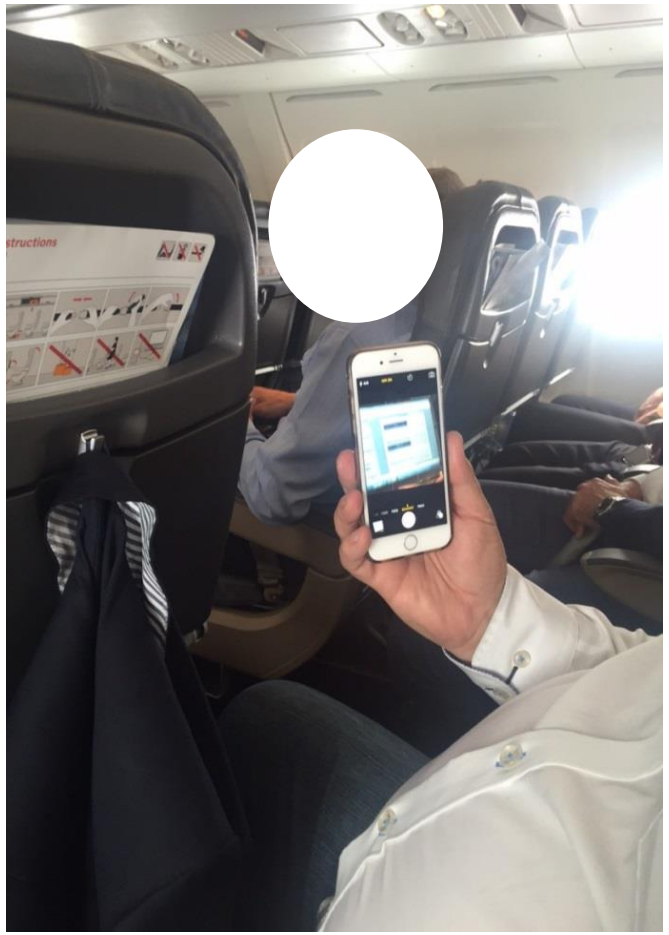
Tweet

Passagier liest mit!

Swiss Flug von London City nach Zürich am 14.5.2015 (17:05)







Wir konnten ohne Probleme die Präsentation lesen. Es war eine M&A Transaktion einer Medical-Company im Auftrag einer Grossbank.

Tipp:

- **Sichtschutzfilter für Notebook-Bildschirm**
- **Geräte «nie» mit Namen und Firma anschreiben!!! → macht nur neugierig!**

Die CEO Phishing-Falle!

Der CEO Fraud ist eine Betrugsmasche, bei der Firmen unter Verwendung falscher Identitäten zur Überweisung von Geld manipuliert werden.

Typischerweise handelt es sich um gut gefälschte E-Mails, die scheinbar von einem Mitglied der Unternehmensführung stammen. Darin wird unter vermeintlich berechtigten Gründen die Überweisung hoher Geldbeträge auf eine ausländische Bankverbindung angewiesen.

Hacker erleichtern Freiburger KMU um eine Million Franken

Unbekannte Hacker haben bei einem Freiburger Unternehmen mehr als eine Million Franken erbeutet. Das Geld wurde nach Polen und China transferiert. Die Konten sind aber bereits wieder aufgelöst worden, wie ein Sprecher der Freiburger Kantonspolizei sagte. Das Geld ist weg, von der Täterschaft fehlt jede Spur.

Ein in Gerlafingen SO ansässiges und schweizweit tätiges Unternehmen sei Ende vergangener Woche gehackt worden, sagte Gallus Risse, Kommunikationschef der Freiburger Kantonspolizei. Von diesem Server aus sei anschliessend ein E-Mail an die im Kanton Freiburg ansässige Partnerfirma verschickt worden.

An das E-Mail war ein Trojaner angehängt. Ein Angestellter der Buchhaltung der betroffenen Firma habe den Anhang geöffnet, obwohl

Die CEO Phishing-Falle!

Tipps

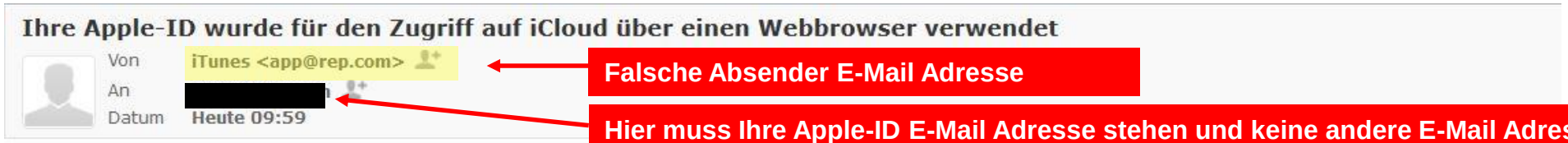
- Es gibt kein Unternehmen, welches die Passwörter ihrer Kunden per E-Mail erfragt.
- Ignorieren Sie E-Mail-Aufforderungen Ihr Passwort zu ändern.
- Öffnen Sie bei **«verdächtigen»** E-Mails nie ein angehängtes Dokument oder Programm und klicken Sie auf keine darin angegebenen Links.
- Geben Sie keine Kundendaten oder Personendaten unberechtigten Dritten Personen bekannt.
- Benutzernamen und Passwörter sind **vertraulich, persönlich und nicht übertragbar.**
- Verwenden Sie für Ihre Arbeit und Privat unterschiedliche Passwörter.
- Bei einer Geld-Transaktion immer telefonisch zurückfragen und sich über die Transaktion informieren.
- Zahlen Sie in keinem Fall eine Lösegeld z.B. in Bitcoins.

Gute CH-Security-Seiten: www.ebas.ch , www.melani.admin.ch , SwissLeak www.swissleak.ch und https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks

Hier können Sie prüfen, ob Ihr Passwort schon gehackt wurde:

https://haveibeenpwned.com/Passwords

Aktuell: Apple Phishing Beispiel



Dieses E-Mail erschreckt Sie als Benutzer einer Apple-ID

Hallo,

Ihre Apple-ID wurde für utilizzatoden Zugriffauf iCloud über einen W… verwendet.

Datum und Uhrzeit: **23 Oktober 2019, 09:39 PDT**

IP-Adresse, Ort: **180.166.56.65, China - Shanghai**

Wenn Sie sich kürzlich bei iCloud angemeldet haben, können Sie d… ignorieren.

Wenn Sie diese änderungen nicht vorgenommen haben oder der meinung sind, dass eine unbefugte Person auf Ihren Account zugegriffen hat, klicken Sie auf die Meine Apple ID.

Mit freundlichen Grüßen,

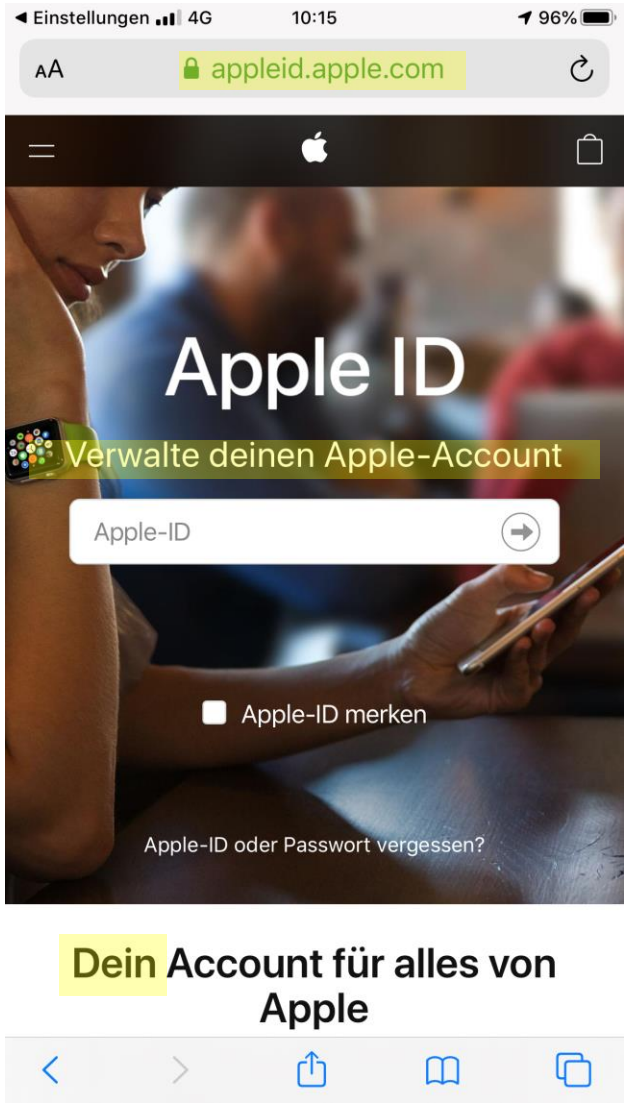
Apple Support

IDApple | Supporto | Normesullaprivacy
Copyright © 2019
Apple Distribution International, Hollyhill Industrial Estate, Hollyhill, Cork, Ireland.
Alle Rechte vorbehalten.

Was ist hier falsch?

- E-Mail an falsche E-Mail Adresse
- Absender «komisch»
- Text-Inhalt «utilizzatoden»???
- Schreibfehler im Text
- Komischer Footer

Aktuell: Apple Phishing Beispiel



Tipp

Immer die URL-Adresse und den Deutschen-Text überprüfen. Apple ist per «Du» und die Phishing-Seite per «Sie».

Lassen Sie sich nicht täuschen und passen Sie auf!

Herausforderungen - Schützen Sie Ihre Werte und Ihr Know-how

- Cloud-Dienste, IoT Geräte, und Abhängigkeiten zu IT-Lieferanten und Schnittstellen
- Keine internen Weisungen und Sicherheitskonzepte
- Kein Notfall- und Krisenkonzept
- Hohe Komplexität – additive Probleme – neue Gesetze (DSG, DSGVO, etc.)
- Hohe Mobilität der Benutzer – Daten überall, zu jeder Zeit und auf jedem Endgerät
- Zuwenig Awareness, viel Halbwissen und Ignoranz
- Mehr und breiter motivierte/ausgerüstete Angreifer
- Mehr vernetze Werte/höheres Schadenpotential
- Ressourcen-Mangel und Schnelligkeit des Wandels

Herausforderungen - Schützen Sie Ihre Werte und Ihr Know-how

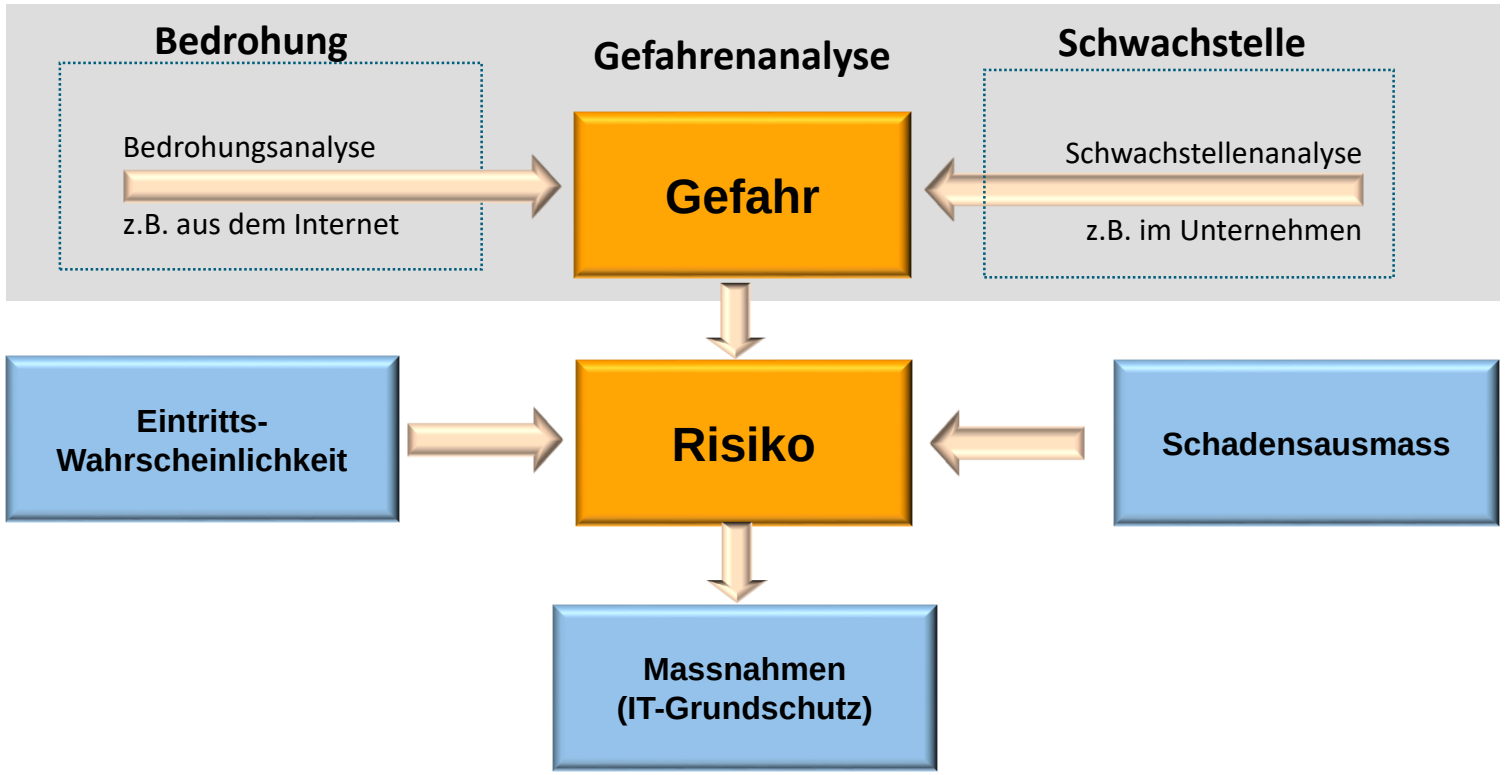
- **Wir fühlen uns zu gut in unserer Komfort-Zone – Schönwetter-Sicht, bei uns passiert das nicht!**
- **Produkte lösen keine Management/Führungsprobleme → Führen & Vorleben**
- **Bevor Sie einen Cloud-Dienst verwenden, klären Sie wie «sicher» dieser Cloud-Service ist.**
- **Haben Sie immer einen Plan «B» und hinterfragen Sie neue Services und Produkte in Bezug auf die Informationssicherheit und den Datenschutz**

Wie sieht es bei Ihnen aus?

- Wie schätzen Sie Ihre eigene IT-Sicherheit / Datenschutz ein?
- Wissen Sie **was** Sie **wie** schützen müssen?
- Hatten Sie schon mal einen Sicherheitsvorfall?
- Haben Sie eine verantwortliche Person für die Informationssicherheit und den Datenschutz?
- Kennen Sie das Verhalten Ihrer Mitarbeitenden in Bezug auf die Informationssicherheit und den Datenschutz?
- Haben Sie Informationssicherheits- und Datenschutz-Weisungen in Ihrem Unternehmen?
- Haben Sie IT-Services ausgelagert? (Outsourcing oder Cloud-Services)
- Haben Sie vertragliche Informationssicherheits- oder Datenschutz-Auflagen von Kunden?
- Haben Sie einen Notfall- und ein Krisenmanagement-Plan?
- Speichern Sie Ihr Daten extern (Offline Backup)?

Wie entsteht ein Risiko?

- Ein Risiko ist die **Gefahr**, dass ein Ereignis eintrifft, das zu einem **Schaden/Verlust** führen kann.
- Oder ist die Gefahr, dass ein Ereignis eintrifft, das die Erreichung der Unternehmensziele **beeinträchtigen/verhindern** kann.



Risiko-Analyse basierend auf ISO 27001/27002

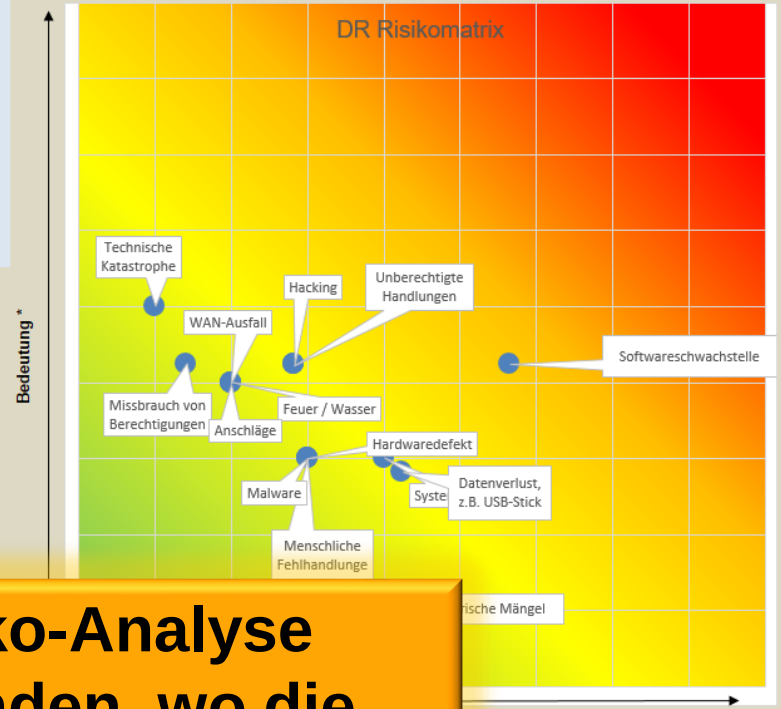
Risiko #	Bedeutung * (B*)	Auftreten * (A*)	Bedeutung (B)	Auftreten (A)	Entdeckungszs zeitpunkt (E)	Risiko-Prioritäts-Zahl (RPZ) = B x A x E	Restrisiko
Systemausfall	3.0	4.0	3	4	1	12	Mittel
WAN-Ausfall	4.0	2.0	4	2	1	8	Mittel
Feuer / Wasser	4.0	2.0	4	2	1	8	Mittel
Technische Katastrophe	5.0	1.0	5	1	1	5	Mittel
Organisatorische Mängel	1.0	3.0	1	3	1	3	Akzeptabel
Menschliche Fehlhandlungen	3.0	3.0	3	3	1	9	Mittel
Datenverlust, z.B. USB-Stick	2.8	4.2	2	3	2	12	Mittel
Hardwaredefekt	3.0	3.0	3	3	1	9	Mittel
Softwareschwachstelle	4.2	5.7	3	4	2	24	Hoch
Hacking	4.2	2.8	3	2	2	12	Mittel
Malware	3.0	3.0	3	3	1	9	Mittel
Missbrauch von Berechtigungen	4.2	1.4	3	1	2	6	Mittel
Unberechtigte Handlungen	4.2	2.8	3	2	2	12	Mittel
Anschläge	4.0	2.0	4	2	1	8	Mittel

Erklärung zur Grafik

Die B= Bedeutung (Schweregrad, Relevanz, Auswirkung) und das A=Auftreten (Eintrittswahrscheinlichkeit) wurden mit der E=Endekungszeitpunkt wie folgt gewogen.
Bedeutung* = B x Wurzel (E)
Auftreten * = A x Wurzel (E)

Mit diesem "Kniff" können die Risikomatrix von einer dreidiemensionen Grafik (B, A,E) in einer zweidiemensionalen Grafik (B*, A*) dargestellt werden.
Die Risikomatrix besteht aus einem 9x9 Raster, damit die RPZ bis Zahlenwert 75 abgebildet werden können.

Risikomatrix



Ich empfehle Ihnen eine Risiko-Analyse durchzuführen um herauszufinden, wo die Gefahren und Bedrohungen speziell für Ihr Unternehmen sind.

Unser Weisungs-Paket für KMU

Die folgenden Weisungen bieten Ihnen einen Basis-Schutz.

- **Leitlinie zur Informationssicherheit und Datenschutz**
- **IT-Nutzungsweisung für alle Mitarbeitenden inkl. Anhang Mobile Datenträger**
- **Security Awareness Flyer**
- etc.

Ziel ist, dass Sie Ihre **Verantwortung** zum Thema Informationssicherheit & Datenschutz dokumentieren und die Weisungen durchsetzen.

Inhalt einer IT-Nutzungsweisung

Inhaltsverzeichnis

Sensibilisierungs-Flyer für die Mitarbeitenden

E-Mails und Anhänge

Viren und sonstige bösartige Software werden am häufigsten verbreitet über
- E-Mails (verseuchte Anhänge)
- USB-Sticks
- Internet-Webseiten

Phishing ist eine Methode von Betrügern, um sich Informationen von ihren Opfern zu beschaffen, die zur persönlichen Bereicherung eingesetzt werden können. Phishing-Angriffe erfolgen oft via E-Mails, in denen Benutzer mit möglichst glaubhaften Geschichten dazu gebracht werden sollen, dem Absender vertraulichen Informationen auszuhändigen.

Das Wichtigste in Kürze:

- ☐ Misstrauen Sie E-Mails, deren Absender Sie nicht kennen oder deren Inhalt Ihnen verdächtig vorkommt.
- ☐ Fahren Sie mit dem Mauszeiger über die Internet-Adresse in der E-Mail, **ohne** zu klicken; so sehen Sie, auf welche Website der Link führt.
- ☐ Öffnen Sie bei verdächtigen E-Mails nie ein angehängtes Dokument oder Programm und wählen Sie keine darin angegebenen Links.
- ☐ Öffnen Sie keine Anhänge, die zwei Endungen aufweisen (z. B. foto.jpg.vbs).
- ☐ Seriöse Unternehmen fragen nie per E-Mail nach persönlichen Daten.
- ☐ Ignorieren Sie E-Mail-Aufforderungen, Ihr Passwort zu ändern.

Sorgfaltspflicht

Ihr Arbeitgeber stellt Ihnen einen gut eingerichteten Arbeitsplatz zur Verfügung, der Ihnen die tägliche Arbeit erleichtern soll. Bitte behandeln Sie die Geräte sorgfältig und mit dem nötigen Respekt.

Bearbeiten Sie Daten, so sind Sie in Ihrem Bereich für die Einhaltung von Datenschutz und Datensicherheit verantwortlich.

Fragen Sie die Security Officer, bevor Sie eine Aktion starten, bei der Sie sich über den Ausgang nicht sicher sind.

Informationen und Kontakt

Bei Fragen:
Wenden Sie sich an den Security Officer.

Für allgemeine Informatikfragen und für die Meldung von verdächtigen Vorfällen:
Wenden Sie sich an den Security Officer
max.sicherheit@firmaxy.ch, +41 41 xxx xx xx

Informationen:
Aktuelle Informationen zum Thema Datenschutz und Informatiksicherheit finden Sie in der **Richtlinie ICT-Nutzung.**

Gesetzliche Grundlage:
Schweizerisches Datenschutzgesetz (DSG)

Informationssicherheit bei Firma Muster AG

Merkblatt für den Alltag
und weiterführende Hinweise

Liebe Mitarbeiterinnen, liebe Mitarbeiter

Der Einsatz von PC, Notebook und anderen Informations- und Kommunikationsmitteln ist für uns alle eine selbstverständliche Notwendigkeit, die aber auch Risiken birgt.

Ihr Sicherheitsbewusstsein und Ihr verantwortungsvolles Verhalten ist die wichtigste Grundlage, dass diese Risiken nicht eintreten.

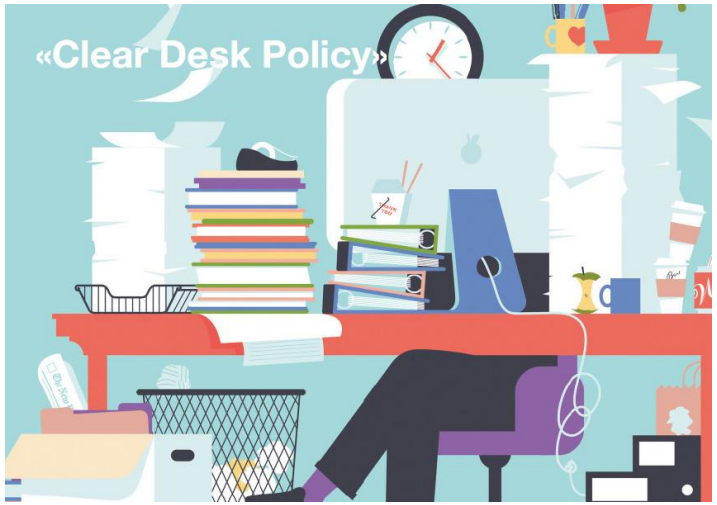
Dieser Flyer soll Ihnen helfen, die Risiken zu erkennen und sich richtig zu verhalten.

Ihr Security Officer
Herr Max Sicherheit
November 2019

Awareness mit «Postkarten»

Effektiv und kostengünstig

SIDLER Information Security



SYNLAB www.synlab.ch

Clear Desk Policy

Ungeschützte Dokumente am Arbeitsplatz können in deiner Abwesenheit sehr leicht von unbefugten eingesehen oder kopiert werden. Verwahre deshalb sensible Dokumente in deiner Abwesenheit an einem sicheren versperrbaren Ort.

SYNLAB ICT-Nutzungsweisung:

- Beim längeren Verlassen des Arbeitsplatzes ist der Arbeitsplatz ordnungsgemäss aufzuräumen.
- Nicht mehr benötigte vertrauliche Dokumente sind sicher zu vernichten (Aktenvernichter). Sie gehören nicht in den Papierkorb und schon gar nicht ins Altpapier.
- Verlasse den Bildschirmarbeitsplatz nie in angemeldetem Zustand. Aktiviere die Bildschirmsperrung (Kennwortschutz). Dies gilt auch für kurze Abwesenheiten wie Toilettenbesuch, Meetings oder Raucherpausen. Bei Mehrbenutzerarbeitsplätzen (LIS-Anwendungen) sind geöffnete Programme mit besonders schützenswerten Daten zu schliessen oder zu sperren, sobald der Arbeitsplatz verlassen wird.
- Bei längerer Abwesenheit und beim Beenden des Arbeitstages ist die Citrix-Session zu schliessen und der Computer ordnungsgemäss herunterzufahren.
- Die Bürotür ist, wenn möglich, abzuschliessen.

März

SYNLAB www.synlab.ch

Patientenrechte

Die Labor-Ergebnisse enthalten Gesundheitsdaten, die das Datenschutzgesetz als besonders schützenswerte Daten bezeichnet. Das eidgenössische Datenschutzgesetz des Bundes gewährleistet den Schutz dieser Daten, die im Grundsatz nur mit der Einwilligung des Patienten (Kunden) bearbeitet werden dürfen. Darüber hinaus bestehen jedoch unter bestimmten Umständen (ansteckende Krankheiten, Verdacht bei Verbrechen oder Vergehen etc.) Melderechte und Meldepflichten, die uns verpflichten oder uns erlauben auch ohne Einverständnis des Patienten Daten weiterzuleiten.

Was ist zu tun?

- Die Angaben für den Labor-Auftrag wurden jeweils beim behandelnden Arzt erhoben inkl. der Einwilligung des Patienten. Wird ein Labor-Auftrag direkt in unsere Laboren entgegengenommen, müssen wir die Einwilligung bei der betroffenen Person selbst einholen. Der Patient hat dabei ein Recht auf Aufklärung über die Art und Weise der beabsichtigten Datenbearbeitung.
- Gib keine Patientendaten oder Personendaten unberechtigten Dritten Personen bekannt. Bei Unklarheiten wende dich an deinen Vorgesetzten.
- Verlangt ein Patient die Löschung oder die Einsicht seiner Befunde (Daten), muss er das entsprechende Antrags-Formular auf unserer Webseite **www.synlab.ch/datenschutz** ausfüllen.

Juni

SYNLAB www.synlab.ch

Bitte klicke keinesfalls auf **Links** oder öffne E-Mail-Anhänge, wenn du deren Herkunft nicht absolut sicher bist oder den Absender nicht persönlich kennst. Du kannst z.B. gebeten werden eine bestimmte Summe auf ein Konto zu überweisen.

Gib deine Passwörter oder Zugangsdaten **niemals** an andere Personen weiter. Niemand, auch kein Mitarbeiter der SYNLAB-IT, benötigt im Support-Fall deine Zugangsdaten.

Antworte niemals auf E-Mails, in denen du nach Passwörtern gefragt wirst, gib Passwörter keinesfalls auf Internetseiten ein, denen du nicht vertraust und reagiere skeptisch gegenüber telefonischen Nachfragen zu Zugangsdaten jeder Art.

Wende dich im Zweifelsfall immer an deinen Vorgesetzten, um Unterstützung zu erhalten.

Teste, ob du eine berechtigte E-Mail von einer Phishing-Mail unterscheiden kannst. Die Hochschule Luzern hat einen Test entwickelt mit dessen Hilfe du die Erkennung verbessern kannst.

Hier geht's zum Test:

August

SYNLAB www.synlab.ch

Social Engineering ist eine verbreitete Methode zum Ausspionieren von vertraulichen Informationen. Angriffsziel ist dabei immer der Mensch. Um an vertrauliche Informationen zu gelangen, wird sehr oft die Gutgläubigkeit und die Hilfsbereitschaft aber auch die Unsicherheit einer Person ausgenutzt. Von fingierten Telefonanrufen, über Personen die sich als jemand anderes ausgeben, bis hin zu Phishing-Attacken, ist alles möglich.

Wie sehen mögliche Social Engineering Angriffe aus?

- Eine Person gibt sich als Techniker aus (z.B. eines Labor Geräteherstellers, eine Telekomanbieters etc.) und versucht so Zugang in unser Labor zu erlangen.
- Du bekommst eine E-Mail, welche dich auffordert einen Link aufzurufen und ein Login zu tätigen oder persönliche Informationen preis zu geben **(Phishing)**.
- Eine Person ruft dich an und gibt vor eine Umfrage durchzuführen, um an sensitive Informationen (z.B. Patientendaten oder zu Sicherheitsmassnahmen etc.) zu gelangen.
- Zu deinem Arbeitsplatz kommt eine Person, die sich als Informatiker ausgibt und dir vorgaukelt, an deinem PC Wartungsarbeiten verrichten zu müssen.

Schütze dich, indem du ...

möglichst wenig persönliche Informationen über dich preisgibst. Insbesondere auf Sozialen Netzwerken wie Facebook, Xing etc. solltest du mit persönlichen Informationen sehr sparsam umgehen. Passwörter grundsätzlich nie einer anderen Person auch deinem Chef oder Systemadministrator bekanntgeben. Ein Passwort gehört dir und nur dir!

Oktober

Unser Phishing Merkblatt

Gib Phishing-Mails keine Chance!
So entlarvst Du Cyberkriminelle

neutrass SIDLER Information Security

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...

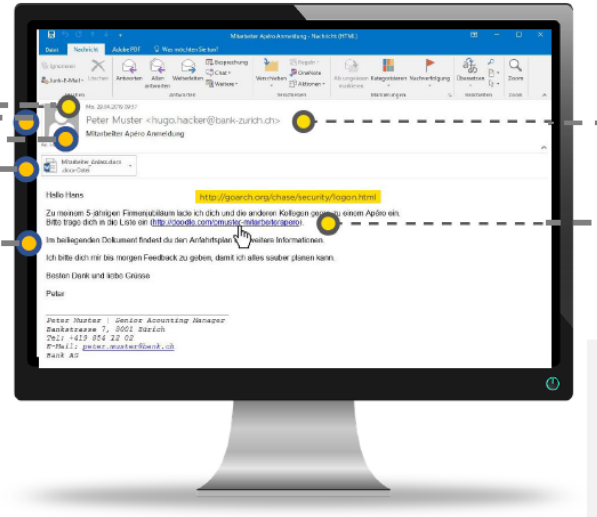
Datum
Wurde die E-Mail zu einer ungewöhnlichen Uhrzeit geschickt (Nacht, Wochenende)?

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 Ihnen 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.

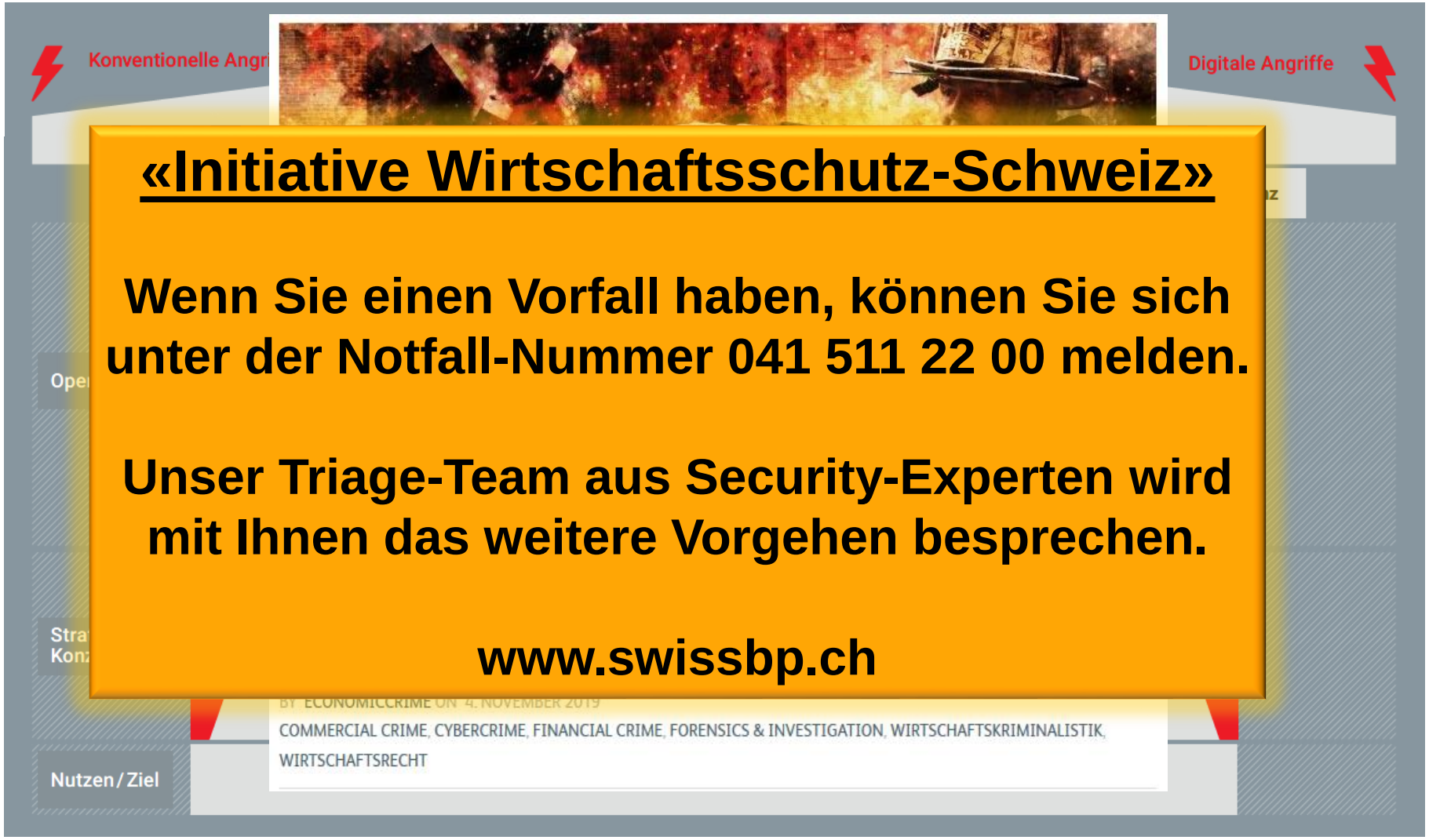
Im Zweifelsfall in einer neuen, separaten E-Mail oder telefonisch beim Absender nachfragen, ob er/sie tatsächlich diese E-Mail geschickt hat.

ONE STEP AHEAD

Version 1.0, November 2019

Unser integraler Sicherheitsansatz

SWISS BUSINESS PROTECTION



«Initiative Wirtschaftsschutz-Schweiz»

Wenn Sie einen Vorfall haben, können Sie sich unter der Notfall-Nummer 041 511 22 00 melden.

Unser Triage-Team aus Security-Experten wird mit Ihnen das weitere Vorgehen besprechen.

www.swissbp.ch

EU-Datenschutz-Grundverordnung (DSGVO/GDPR)

SIDLER Information Security

Jedes Unternehmen, das personenbezogene Daten von in einem EU-Mitgliedstaat wohnhaften Bürgern **speichert oder verarbeitet**, muss die DSGVO einhalten, auch wenn es keinen eigenen Sitz in der EU hat. Unternehmen, die eines oder mehrere der folgenden Kriterien erfüllen, müssen die Verordnung einhalten:

- ein Sitz in einem Mitgliedstaat der EU
- kein Sitz in einem Mitgliedstaat der EU, aber Verarbeitung personenbezogener Daten von in der EU wohnhaften Bürgern

Wenn also Ihr Unternehmen in der EU tätig ist oder Mitarbeiter oder Kunden aus der EU hat, müssen Sie ab dem **25. Mai 2018** die DSGVO einhalten.

Die alte Welt

- EU-Datenschutz vor der digitalen Welt (veraltet)
- Keine Audits und nur wenige Untersuchungen
- Wurde nicht konsequent in Europa umgesetzt
- Kleine Bussen, wenn überhaupt!

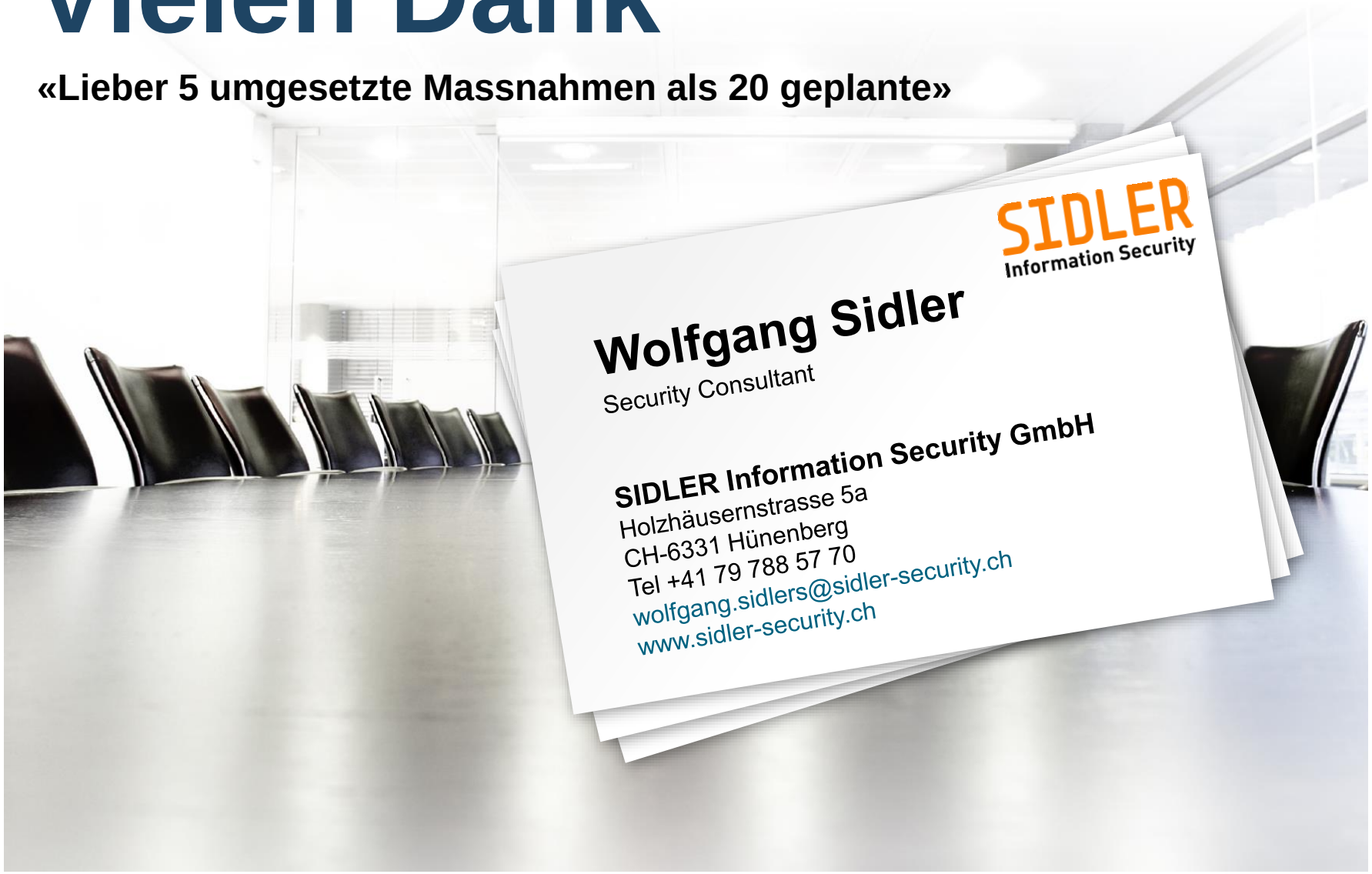
Die neue Welt - keine Änderungen in Bezug auf den IT-Grundschutz, aber:

- Bussen bis 4% des globalen Unternehmens-Umsatz
- EU Bürger haben neu viel mehr Rechte
- Nachweispflicht der Umsetzung (Compliance)

DSGVO = Datenschutz-Grundverordnung
GDPR = EU General Data Protection Regulation

Vielen Dank

«Lieber 5 umgesetzte Massnahmen als 20 geplante»



SIDLER Information Security

ÜBER 10 JAHRE FÜR SIE DA

SWISS BUSINESS PROTECTION

www.swissbp.ch

FAZIT und Tipps (1/3)

- Achtung bei der Verwendung von Google Translator oder DeepL (wird alles zwischengespeichert und analysiert) Fall einer Bank mit Kundennamen.
- Sicherheit ist immer eine Abwägung zwischen Sicherheit und Bedienbarkeit (Usability)
- Bewerbungsmail mit Anhängen vermeiden. Stattdessen ein HR Portal für den Upload des CV etc. auf der Firmenwebseite
- Phishing Mails werden zunehmen und noch besser werden – Awareness!!!
- Beispiel: gehackter Exchange Mail Server (Eine Kopie der E-Mails ging an den Mitbewerber)
- Benutzerberechtigungen jedes Jahr prüfen (Lehrling hat meistens mehr Rechte als der CEO!) Ein- und Austritts-Checkliste erstellen.
- Netzwerk mit IoT Geräten (Produktion, Lager, Labor, etc.) immer vom Office Netzwerk trennen
- Ein Cloud-Konzept bzw. Weisung erstellen – immer ein Sicherheitskonzept inkl. Risiko-Analyse für jede Cloud-Anwendung erstellen.
- Bei einer Cloud-Lösungen müssen Sie achten, das der Schlüssel bei Ihnen bleibt (HSM)
- Wichtig ist, dass Sie Ihre Lieferanten kennen. Speziell jene mit einer online-Anbindung für Wartung etc.)

FAZIT und Tipps (2/3)

- 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!
- Die Mitarbeitenden auf allen Stufen regelmässig sensibilisieren – geht auch kostengünstig mit Postkarten
- Sie benötigen ein Minimum an internen Weisungen mit entsprechenden Sanktionen. Sonst hören Sie: Das wurde mir nie gesagt …. Das wusste ich nicht …
- Haben Sie einen Notfallplan für ein Ereignis oder eine Krise bereit «Plan B)!
- Verschlüsseln Sie die Festplatten Ihrer Notebooks. Das gibt auch den Benutzer die Sicherheit bei einem Verlust des Notebooks.
- Haben Sie immer ein Offline (Offsite) Backup Ihrer Daten
- Halten Sie Ihre Programme immer aktuell (Patch-Management)
- Setzen Sie unterwegs beim Notebook immer eine Sichtschutzfolie ein

FAZIT und Tipps (2/3)

- Bei einer «komischen» Geld-Transaktion immer telefonisch zurückfragen und sich über die Transaktion informieren.
- Achten Sie darauf, dass es in Ihrem Unternehmen keine Schatten-IT gibt (wild installierte WLAN-AP, MFP, etc.)
- Wenn Sie mit einer Webseite online gehen, bitte vorher von Spezialisten (Ethical Hacker) penetrieren lassen, um die Schwachstellen zu finden und zu beheben
- Verwenden Sie immer «starke» Passwörter – min. 12 Zeichen und mit Sonderzeichen
- Ändern Sie bei allen IT-Geräten immer das Default-Passwort
- Achten Sie darauf, dass in Ihrem Unternehmen vertrauliche Dokumente «sicher» vernichtet werden (Shredder oder Dokumenten-Vernichtungs-Service)

Auszug Referenzen

SIDLER Information Security

KANTON LUZERN Finanzdepartement Dienststelle Personal

KANTON LUZERN Staatskanzlei

Gemeinde EMMEN

Dienststelle Informatik informatik.lu.ch

Stadt Zürich Organisation und Informatik

Almo personal ag

prema swiss precision cash handling systems

delacruz beranek RECHTSANWÄLTE • ATTORNEYS AT LAW

Zwicky Windlin & Partner Rechtsanwälte Urkundspersonen

AW Amédéo Wermelinger Kanzlei am Bahnhof

Heller Anwaltskanzlei

NICK TREUHAND AG

INTEGRA AGP LUZERN Akademie für Gesundheit & Persönlichkeitsbildung

PILATUS

komax

Landis+Gyr manage energy better

perlen papier ag

CONTRAFEU

NORILSK NICKEL

APOSTROPH ÜBERSETZUNGEN & LOKALISIERUNG

UBS

Aargauische Kantonalbank

Volvo Trucks SCHWEIZ

Opacc Extended Enterprise Software

SWISS FORT KNOX

SIAG

KEYNET ICT SOLUTION

MUSAR ARCHITEKTEN

SYNLAB

Geistlich Pharma

CSS Versicherung

HOFFMANN NEOPAC TINS AND TUBES

EUROIMMUN

Clever.Care