Cyber-Schutz

FÜR IHR UNTERNEHMEN

Reale Hilfe für virtuelle Probleme

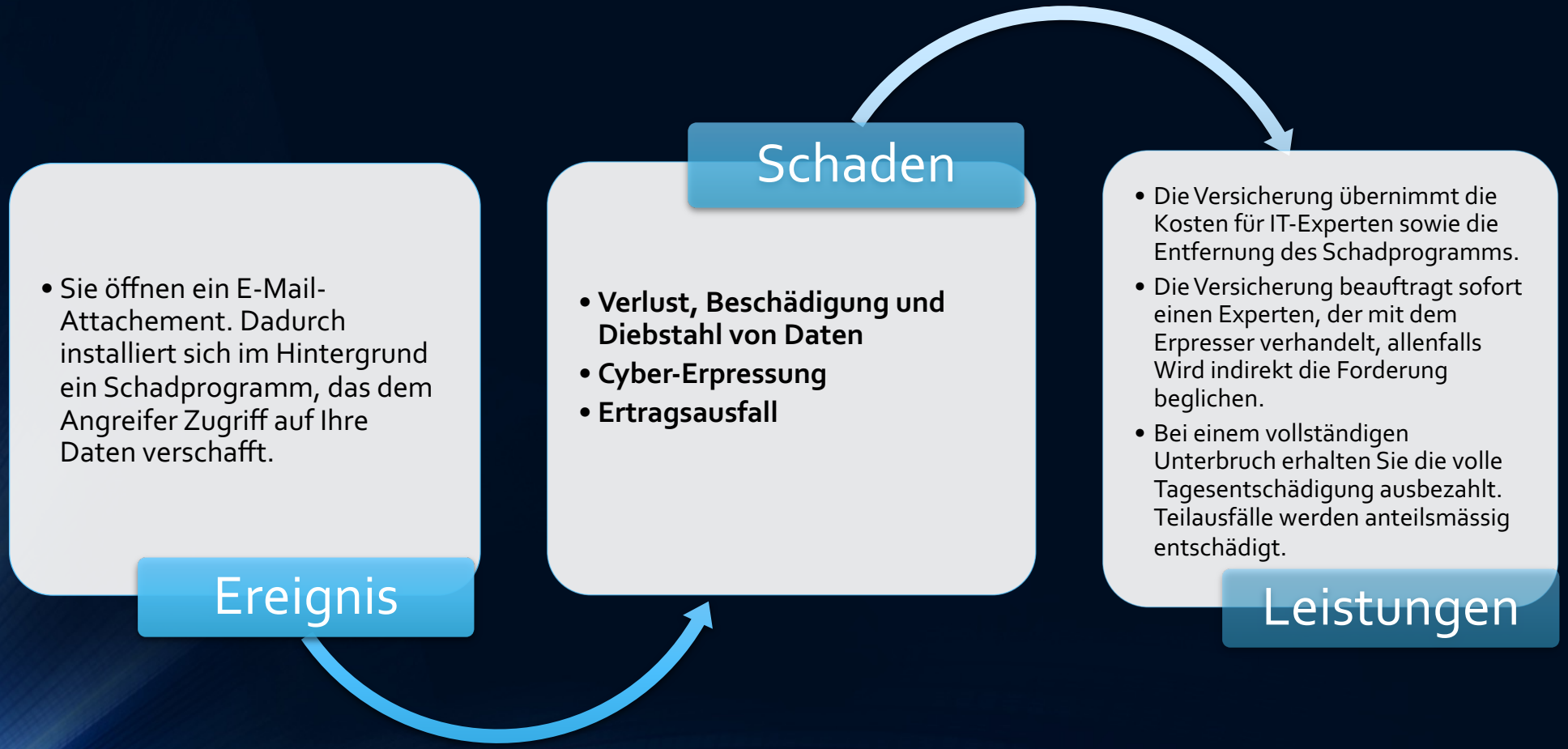
Die digitale Welt birgt Risiken. Das Internet öffnet leider nicht nur den Versicherungsgesellschaften die digitale Tür zur Welt, sondern auch unerwünschten Gästen. Gemäss einer Studie der KPMG, einer der führenden Wirtschaftsprüf- und Beratungsunternehmen, wurden über 50% der Unternehmen in der Schweiz Opfer einer Cyber-Attacke.

eReSTe VersicherngsBroker AG berät Sie gerne, um eine massgeschneiderte Lösung anzubieten.

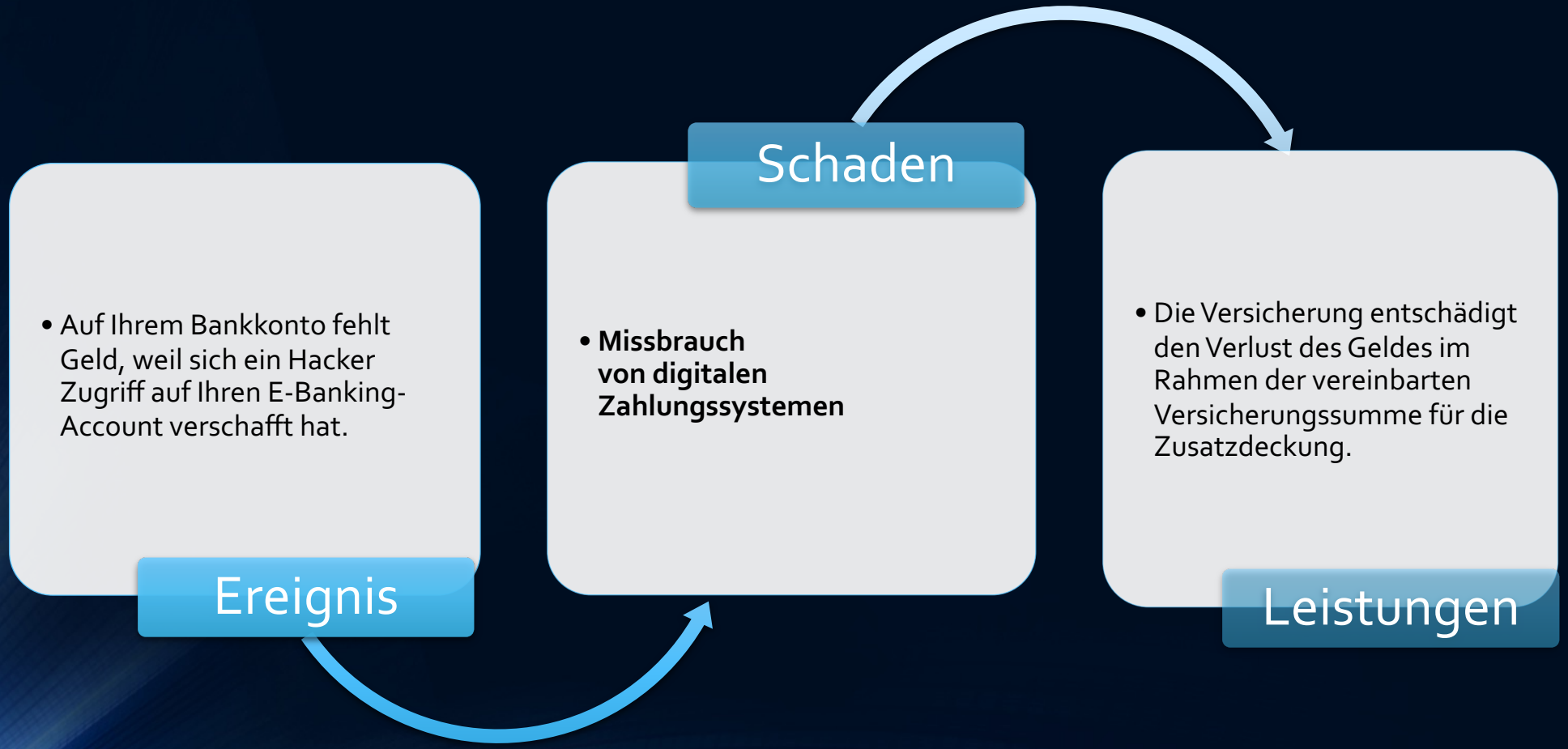
Cyberversicherung kann folgendes abdecken

- **Cyber-System- und Datenwiederherstellung**
- **Cyber-Krisenmanagement**
- **Cyber-Haftpflicht**
- **Cyber-Rechtsschutz**
- **Cyber-Betriebsunterbruch und Mehrkosten**
- **Cyber-Crime**

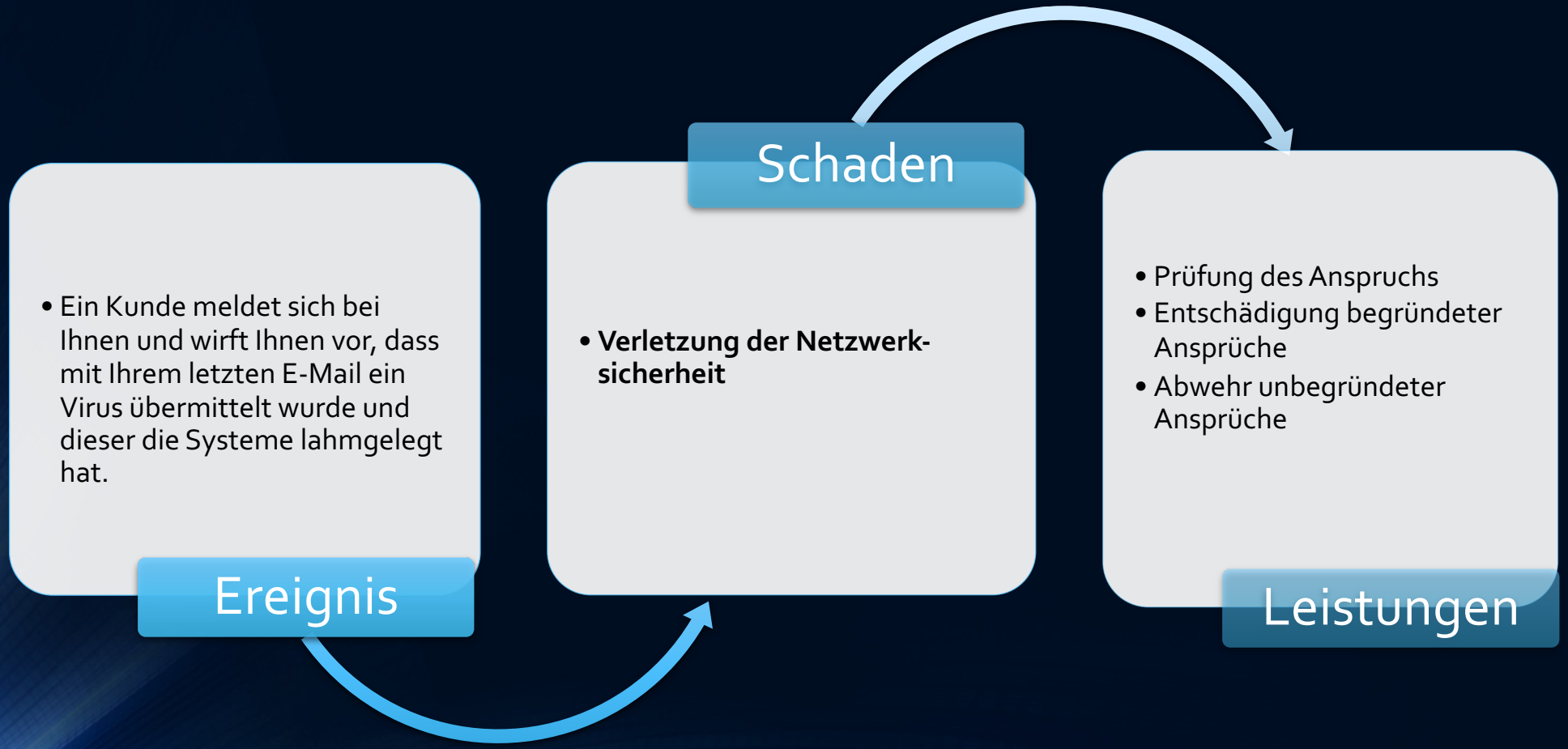
Einige Praxis-Beispiele



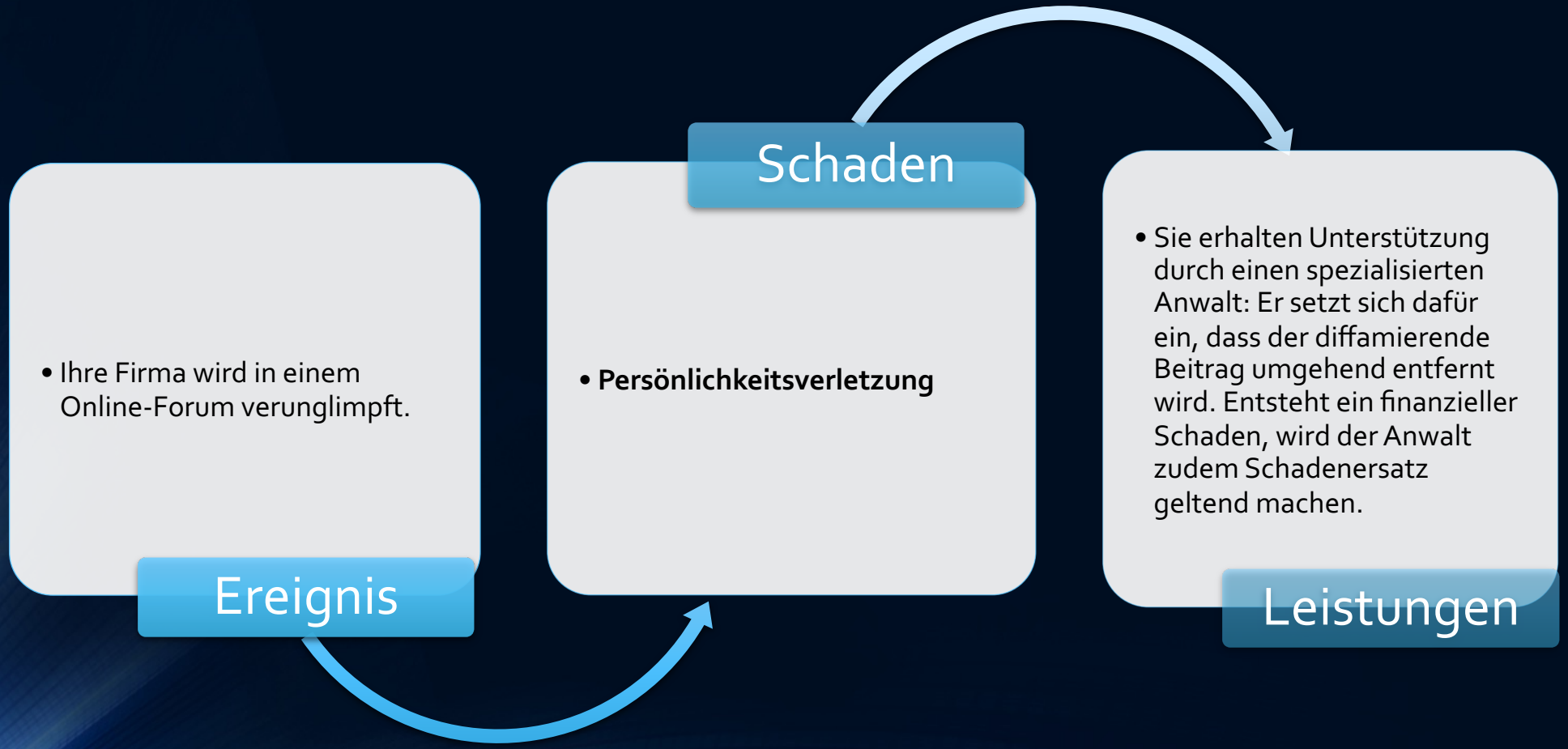
Einige Praxis-Beispiele



Einige Praxis-Beispiele



Einige Praxis-Beispiele



Tipps

Tipp 1 – Bewahren Sie Datenträger sicher auf

- Erstellen Sie ein lückenloses Backup-Konzept: Legen Sie schriftlich fest, wer für die Datensicherung zuständig ist. Werden Sie sich bewusst, welche Art Daten Sie haben, wo diese gespeichert werden und wie kritisch diese für die Geschäftstätigkeit sind.
- Stellen Sie sicher, dass die Backups erfolgreich durchlaufen. Zum Beispiel mit einer Meldung an den Administrator.
- Bewahren Sie die Datenträger an vor äusseren Einflüssen geschützten Orten auf. Wenn möglich speichern Sie die Backup-Medien ausserhalb des produktiven Netzes bei einem externen Unternehmen oder auf einem Cloud-Server.
- Sichern Sie nach dem Motto: «Doppelt gesichert hält besser!»

Tipp 2 – Überprüfen Sie Ihre Systeme regelmässig

- Zur Datensicherung gehört die regelmässige Kontrolle der Backups auf Vollständigkeit und Lesbarkeit. Überprüfen Sie mindestens jährlich (bei Technologiewechsel öfter), ob alle eingesetzten Backup-Mechanismen korrekt funktionieren. Denn: Jede Sicherung ist nutzlos, wenn die Daten nicht richtig auf das Backup-Medium übertragen oder wiederhergestellt werden können.
- Sie können Geräte und Systeme selber warten oder die Arbeit an Partner übergeben. Achten Sie auf vertrauenswürdige Unternehmen und gewähren Sie nur beschränkte Zugangs- und Zugriffsrechte (zum Beispiel mit einer Vertraulichkeitsvereinbarung).
- Überarbeiten Sie Ihr Backup-Konzept regelmässig. Denken Sie dabei an Systemanpassungen, neue Applikationen oder andere Veränderungen.

Tipps

Tipp 3 – Planen Sie regelmässige Backups

- Wie häufig Sie Ihre Daten sichern sollten, richtet sich nach Grösse und Tätigkeit Ihres Betriebs. Mindestens einmal wöchentlich sollte jedes Unternehmen seine Daten sichern.

Als Best-Practice Beispiel empfehlen wir:

- Machen Sie von Montag bis Donnerstag je ein *Tages-Backup* auf einem eigenen Speichermedium. Die Tages-Backups werden nach einer Woche überschrieben. Aufbewahrung: ausserhalb des Serverraums.
- Erstellen Sie freitags ein *Wochen-Backup* auf einem separaten Speichermedium. Es wird nach einem Monat überschrieben. Aufbewahrung: ausserhalb des Betriebs.
- Machen Sie am Monatsende das *Monats-Backup.* Es wird nicht überschrieben. Aufbewahrung: ausserhalb des Betriebs.
- Ende Jahr erstellen Sie das *Jahres-Backup.* Es wird nicht überschrieben. Aufbewahrung: ausserhalb des Betriebs.

Die 3-2-1 Backup-Regel

- *Beachten Sie zur Datensicherung:*
- 3 Erstellen Sie im Minimum drei Sicherungskopien.
  2 Verwenden Sie mindestens zwei verschiedene
- Datenträger.
  1 Bewahren Sie ein Backup ausser Haus auf.

Tagtägliche Angriffe auf Schweizer Firmen

Partner von BILANZ

BUSINESS INNOVATION 2020

In den Fängen der Datendiebe

Lesezeit: 4 Minuten

Erpresser-Software Sie kommt ganz unscheinbar daher, verursacht oft aber massive Schäden. Wer sich den Cyberkriminellen nicht ausliefern will, muss auf ihre Angriffe vorbereitet sein.

Von **Volker Richert**
am 17.09.2020

Lange war von Datenrettung hauptsächlich die Rede, wenn durch physisch beschädigte Hardware Datenverluste drohten. Wichtige Informationen auf Servern, Smartphones, USB-Sticks oder anderen IT-Komponenten mussten wiederhergestellt werden.

Inzwischen sind durch Hackerangriffe ganz andere Bedrohungsszenarien virulent geworden und deutlich stärker als bisher in den Fokus gerückt. Es sind immer professioneller betriebene Angriffe mit spezieller Schadsoftware, die nicht selten Millionenschäden verursachen. Unternehmen und öffentliche Institutionen werden durch Betriebsunterbrüche oder Reputationsschäden im Kerngeschäft getroffen. Ablesen liess sich das zuletzt an der rasanten Zunahme [illegible] Erpressungen.

Luzerner Zeitung

CYBERKRIMINALITÄT

Die internationale Cybermafia: Hackerangriff auf Firmen nehmen in der Schweiz bedrohliche Züge an

Huber+Suhner musste die Produktion stilllegen, der Medienkonzern TX Group erlitt einen teilweise erfolgreichen Angriff: Die Gefahr von Cyberangriffen auf Unternehmen und kritische Infrastruktur steigt.

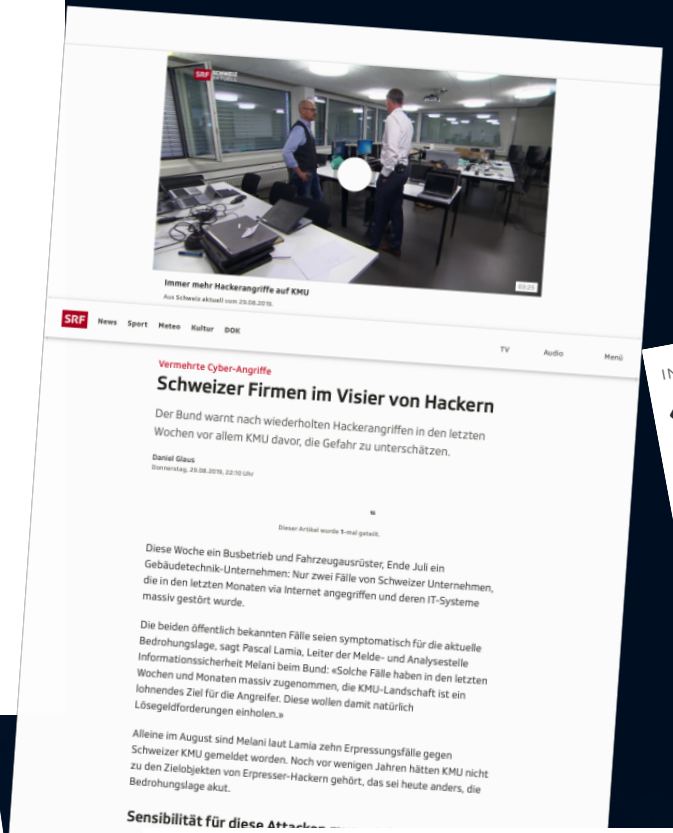
Christian Mensch
16.01.2021, 05.00 Uhr

Keystone

Der Zürcher Medienkonzern TX Group wurde Opfer von Cyberkriminellen.

Wenn die Systeme Alarm schlagen, ist es häufig zu spät. Der Virus hat sich schon vor Tagen oder gar schon vor Monaten eingenistet. Als Schläfer orientiert er sich in der Umgebung, eruiert Schwachpunkte, öffnet Hintertüren, saugt Daten ab oder installiert weitere Schadsoftware.

Im November war ein solcher Angriff beim Medienkonzern TX Group teilweise erfolgreich. Eine toxische Software legte die Verbindungen in der IT-Infrastruktur lahm. Abonnenten konnten ihre E-Papers nicht laden. Websites waren zeitweise nicht erreichbar. Der erkennbare Schaden hielt [illegible] Grenzen, die Angriffe hätten abgewehrt werden können, teilte das



Startseite > Geschäftskunden > KMU > KMU-Fokus > KMU-Fokus 01/2021 > Cyberangriffe auf KMU nehmen zu

Cyberangriffe auf KMU nehmen zu

Viele KMU haben gerade andere Prioritäten als die IT-Sicherheit. Doch die Gefahren werden komplexer und vielfältiger, die Risiken höher und die Kriminellen immer professioneller. Welche Bedrohungen sind besonders aktuell? Ein KMU berichtet über seine Erfahrungen und unser Chief Information Security Officer Philipp Rütsche gibt wertvolle Tipps.

Partner von BILANZ

INTERNET

«In der Schweiz nehmen Cyber-Angriffe massiv zu»

Lesezeit: 4 Minuten

Reto Häni ist langjähriger Fachmann für Cyberrisiken. Er erklärt die Folgen der WannaCry-Attacke, warum so viele Firmen schlecht geschützt sind und sagt, was die Schweiz verbessern muss.

Von **Tim Höfinghoff**
am 15.05.2017

Herr Häni*, die globale WannaCry-Attacke hat die Schweiz anscheinend weniger stark getroffen – können wir uns beruhigt zurücklehnen?

Das sollten wir sicherlich nicht machen. Die Schadsoftware mit dem Namen WannaCry hat weltweit viel Schaden angerichtet. Auch die Schweiz ist betroffen, wenn auch nicht so stark wie zum Beispiel Grossbritannien. Was am vergangenen Wochenende passiert ist, waren aber nur die ersten Wellen. Ich gehe davon aus, dass es noch weitere Angriffe in diesem Stil geben wird.

Wie ernst ist die Lage?

Es zeigt, dass viele Schweizer KMU zu wenig vorbereitet sind in Sachen Cybersecurity. Dieser Angriff ist erst der Anfang eines sich zunehmend verschärfenden Problems. Immerhin ist die Schweiz bisher zwar nicht direkt angegriffen worden. Aber das heisst nicht, dass sich das nicht ändern wird. In Zukunft kann es auch gezieltere Angriffe auf Schweizer Internet-Domains geben, wie das auch schon früher eingeschränkt der Fall war.

Partner von BILANZ

NEWS

Millionenschaden: Metall Zug wird Opfer eines Cyberangriffs

Lesezeit: 1 Minute

Der Vorfall ereignete sich im April in den USA: Wegen des Angriffs der Cyberkriminellen wurden eine Zahlung auf ein falsche Konto überwiesen.

Veröffentlicht am 17.06.2020

Der Industriekonzern Metall Zug ist in den USA Opfer eine Cyberangriffs geworden. Hacker infiltrierten im April den Geschäftsbereich Medical Devices. Wegen des Cyberangriffs wurde eine interne Zahlung auf ein falsches Konto überwiesen.

FRAGEN?

Ich habe bereits einen IT-Dienstleister oder einen IT-Verantwortlichen, mit dem ich sehr zufrieden bin, brauche ich trotzdem eine Cyberversicherung?
Ein guter IT-Fachmann ist in der heutigen Zeit immens wichtig. Bei einer Cyber-Attacke steht Ihnen dieser sicher sofort zur Verfügung. Seine Zeit wird er Ihnen in Rechnung stellen, die dann Ihre Versicherung bezahlen würde. Ausserdem haben Sie dann einen Partner, der auf IT-Security spezialisiert ist, was ein entscheidender Vorteil bei der Bewältigung einer Cyber-Attacke sein kann.

Mein Betrieb ist zu klein, um angegriffen zu werden? (Ich habe nur wenige PC's)
Kann Ihr Betrieb ohne IT weitergeführt werden? Wenn Sie diese Frage mit "Nein" beantworten müssen, dann empfehle ich Ihnen den Abschluss einer Versicherung, welche Ihnen die Mehrkosten und den entgangenen Gewinn absichert. Gerade auch kleine KMU werden in der letzten Zeit immer wieder angegriffen. Sie sind in der Regel einfachere Ziele als grosse Unternehmen mit einer eigenen IT-Abteilung.

Ich habe einen aktuellen Virenschutz und eine aktuelle Firewall, das genügt doch?
Der neuste Schutz wehrt sämtliche bekannten Angriffsmethoden ab und ist darum unerlässlich. Es gibt aber immer wieder neue Angriffsmethoden, die nicht entdeckt werden. Darum gibt es keinen 100% Schutz. Wenn ausserdem jemand von innerhalb des Netzwerkes auf einen schädlichen Anhang klickt, dann nützt auch der beste Schutz nichts.

Ich habe alle Daten in einer sicheren Cloud abgespeichert, da kann doch nichts passieren?
Der Cloud-Anbieter sichert sich vertraglich Ihnen gegenüber ab so, dass er im Falle eines Datenverlustes nicht haftbar gemacht werden kann. Wenn die Daten auf der Cloud verschlüsselt werden, dann ist Ihr Betrieb ebenso beeinträchtigt, wie wenn die Daten bei Ihnen auf dem Server liegen würden. Eine Cyberversicherung deckt Ihnen die entgangenen Gewinne auch dann, wenn die Daten auf einer Cloud liegen.

FRAGEN?

Meine Daten werden extern gesichert, das ist doch besser?
Manche Würmer nisten sich auf Ihren Systemen ein und warten, bis die nächste Datensicherung ausgeführt wird. Sie sichern dann quasi den Wurm mit. Sobald sich dieser überall eingenistet hat, aktiviert er sich und verschlüsselt alle Daten - auch diese auf dem externen Backup.

Mein Betrieb läuft auch ohne EDV weiter?
Die Erfahrung zeigt, dass durch eine Cyberattacke die EDV nicht selten über längere Dauer beeinträchtigt oder ausgeschaltet wird und dies den Geschäftsgang der allermeisten Betriebe erheblich einschränkt. Können Sie beispielsweise wirklich ohne Zugriff auf ihr System Ende Monat die Löhne auszahlen?

Ich mache doch ein Backup, genügt das nicht?
Ein korrektes Backup ist essentiell. Haben Sie auch schon versucht dieses wieder einzuspielen bzw. wurde es auf die Korrektheit getestet? Trotzdem, auch mit einem guten Backup entstehen Folgekosten für das komplette Neuaufsetzen des Systems, Erteilen von Berechtigungen, etc. erst ganz am Schluss kann ein Backup wieder aufgespielt werden.

Für diese Schäden haftet doch die Bank? (Hacking E-Banking)
Nein, in den allermeisten Fällen haftet die Bank nicht. Sie haftet nur dann, wenn die Bank eine Schuld trifft. Wenn die Hacker über Ihren PC sprich über Ihr e-banking Geld transferieren, trifft die Bank in den meisten Fällen keine Schuld. Bezahlt die Bank den Verlust trotzdem ist es in der Regel aus Kulanz. Es sind auch Fälle bekannt, wo die Bank jegliche Zahlung verweigert hat.

eReSTe VersicherungsBroker AG

Industriestrasse 18

8108 Dällikon

Telefon 044 847 40 50

info@ereste.ch