Die ITeen-Schmiede
IT-Solutions by Marco Rukwid

»Do hört dr Schbaß uff!!«

IT-Sicherheit: Wir haben das Wichtigste für Sie zusammengefasst.

Kennen Sie das?

- Sie sorgen sich um potenzielle Sicherheitslücken und Datenverlust
- Sie fürchten Hackerangriffe oder Imageschäden
- Die Bedrohungen durch Cyberkriminelle bereiten Ihnen schlaflose Nächte
- Es fehlt Ihnen der Überblick und die Zeit für Analysen
- Die ständige Angst vor existenzbedrohenden Folgen raubt wertvolle Energie für das Tagesgeschäft und blockiert Ihren Fortschritt.

Wünschen Sie sich auch...

- Klarheit über mögliche Schwachstellen in Ihrer IT-Landschaft
- konkrete Empfehlungen für wirkungsvolle Schutzmaßnahmen
- eine bedarfsgerechte Beratung durch erfahrene Experten
- Gewissheit über die Sicherheit sämtlicher Systeme
- einen freien Kopf für Ihr Kerngeschäft

Schützen Sie Ihre Komponenten, Daten und Kommunikation vor Angriffen.

Die Frage ist nicht, ob Sie angegriffen werden, sondern wann!

IT-Sicherheit ist Chefsache!

Die Geschäftsführung muss das Thema ernst nehmen. Die beste IT-Sicherheit bringt nichts, wenn der Mensch Fehler macht.

Hacker greifen Unternehmen mit immer raffinierteren Methoden an. Viele der Attacken lassen sich mit technischen Mitteln abwehren. Wie Sie sich auf den IT-Ernstfall vorbereiten. 86 Prozent der teilnehmenden Unternehmen beklagen in der Umfrage »Wirtschaftsschutz 2021« des Digitalverbandes Bitkom Schäden durch Cyberangriffe. Unfassbare 223.5 Mia. Euro schätzt der Verband die Gesamtkosten.

Mit den richtigen technischen Einstellungen und mit organisatorischen Maßnahmen, wie der Beschränkung von Zugriffsrechten, lassen sich viele der typischen Angriffe abwehren.

Unternehmer sind den Hackerbanden nicht vollkommen wehrlos ausgeliefert:

Deshalb ist es wichtig eine IT-Sicherheitskultur im Unternehmen zu etablieren, denn Betrüger wissen jede menschliche Schwächen auszunutzen.

Jeder Unternehmer sollte den Cyber-Ernstfall einplanen und firmeninterne Richtlinien für ein IT-Notfallmanagement ausarbeiten.

Der Unternehmer muss sein Unternehmensnetzwerk nicht selbst administrieren – sollte aber wissen, wie die Bausteine ihrer Unternehmens-IT zusammenhängen, um auch in einer IT-Krise die richtigen Entscheidungen treffen zu können.

Verschiedene Arten von Angriffen:

- **Ransomware:** Daten werden verschlüsselt und Lösegeld verlangt
- **Spyware:** Späht Daten und Nutzer aus.
- **Phishing:** Versucht von Beschäftigten mit gefälschten Mails Daten wie Passwörter zu entlocken oder Maleware einzuschleusen.
- **CEO-Fraud:** Betrüger geben sich in Mails oder am Telefon z.B. als Geschäftsführer aus, um Überweisungen zu erwirken.
- **Distributet Denial of Service (DDoS):** Attacken überlasten Server mit massenhaften Anfragen und legen sie so lahm.
- **Defacing:** Betrüger verändern Inhalte auf Websites

Die ITeen-Schmiede
Inh. Marco Rukwid
An der Technologiewerkstatt 1
72461 Albstadt
Telefon 0 74 32 – 13 097 0
E-Mail hallo@dieiteenschmiede.de
www.dieiteenschmiede.de

Die ITeen-Schmiede
IT-Solutions by Marco Rukwid

Diese Checkliste rettet Ihr Unternehmen!

1. Die Relevanz erkennen und dem Team vermitteln

Die IT ist in den allermeisten Betrieben so zentral, dass sie bei einem Angriff keine Dienstleistung mehr anbieten können, Produktionsstraßen still stehen oder Kundendaten weg sind – das könnte im Nachgang zu einem Datenschutzproblem werden. Wer z.B. einen Diebstahl von Kundendaten nicht innerhalb von 72 Std. meldet, dem drohen Bußgelder.

- **Eignen Sie sich IT-Grundwissen an.**
- **Vertrauen Sie einem IT-Dienstleister, der Sie unabhängig berät.**
- **Machen Sie konkrete Pläne, welche IT-Maßnahmen Sie bis wann umsetzen, z.B. von der digitalen Auftragerstellung bis zur Installation einer Überwachungskamera auf dem Betriebsgelände.**

Die Bedeutung von IT-Sicherheit regelmäßig dem Team zu kommunizieren und auch in aller Klarheit verdeutlichen was im Betrieb konkret für Schutzmaßnahmen unternommen wurden.

z.B. Welches System? Wer ist Administrator und wer organisiert den Workshop in Sachen Pishing und Cybersicherheit im Tagesgeschäft?

2. Analysieren, wo Risiken lauern

- **Erstellen Sie eine Liste, welche IT-Geräte im Unternehmen im Einsatz sind. Achten Sie dabei auch darauf, was miteinander vernetzt ist – und sich eventuell durch Segmentierung trennen ließe.**
- **Erfassen Sie auch die Software und welche Beschäftigten die einzelnen Programme nutzen.**
- **Achten Sie darauf, wo Ihre Systeme besonders angreifbar sind.**

3. Die »Kronjuwelen« Ihres Unternehmens identifizieren

- **Überlegen Sie, welches die zentralen Daten und Prozesse im Unternehmen sind.**
- **Kümmern Sie sich als Erstes um die Sicherheit dieser »Kronjuwelen«.**

4. Zugriffsrechte beschränken und Software aktualisieren.

86 Prozent der Cyberangriffe könnten mit vier einfachen Sicherheitskontrollen vermieden werden, schätzt das Bundesamt für Sicherheit in der Informationstechnik (BSI):

- **Nicht jeder im Unternehmen sollte Sicherheitseinstellungen ändern können,**
- **nicht jeder sollte Zugriff auf andere Benutzerkonten haben.**
- **nicht jeder sollte auf alle Dateien zugreifen können,**
- **Administratorrechte sollten grundsätzlich eingeschränkt und den Fachkollegen vorbehalten werden.**

– Dokumentieren und beschränken Sie die Zugriffs- und Administratorrechte innerhalb der Belegschaft.

– Im Betrieb ist jemand dafür zuständig, dass Software-Updates und -Aktualisierungen durchgeführt werden.

5. Checken Sie Ihre Firewall und Ihren Virenscanner

Kleinere Betriebe ohne Produktion sind mit der Kombination aus Firewall und Antivirussoftware gut aufgestellt. Es gibt auch höherwertige Firewalls, die Contentprüfungen vornehmen und Alarm schlagen, wenn Angriffsmuster auftauchen.

Virenscanner dienen dazu, den Computer regelmäßig auf Schadsoftware zu untersuchen und Alarm zu schlagen, wenn sie welche finden.

- **An jeder Schnittstelle vom Unternehmensnetzwerk zum Internet kontrolliert eine Firewall den Zugang.**
- **Auf jedem Gerät, das auf das Internet zugreifen kann, ist ein Virenschutzprogramm installiert.**
- **Der Anti-Viren-Schutz sollte regelmäßig upgedatet werden.**

6. Mehr Schutz für den DNS Ihrer Internetseite

- **Informieren Sie sich, wie Ihr DNS-Provider seine Server schützt**
- **Recovery Plan mit Notfallnummern und Anweisungen, was im Fall eines Cyber-Angriffs zu tun ist. Wichtige Dokumente, die wir auch ohne Server nutzen könnten, auf externen Festplatten zusätzlich speichern.**

Die ITeen-Schmiede
Inh. Marco Rukwid
An der Technologiewerkstatt 1
72461 Albstadt
Telefon 0 74 32 – 13 097 0
E-Mail hallo@dieiteenschmiede.de
www.dieiteenschmiede.de

7. Die Gefahr im Mailpostfach minimieren.

Im März 2021 bekamen mehr als 9.000 Unternehmen Post vom BSI, weil ihrer Exchange-Server – und damit ihr gesamtes Unternehmen – in Gefahr waren. Eine chinesische Hackergruppe hatte mehrere Sicherheitslücken in der Microsoft-Software ausgemacht. Über 30.000 Organisationen waren von dem Cyberangriff betroffen. Experten gehen davon aus, dass noch immer nicht alle Unternehmen, die notwendigen Updates erledigt haben, um Sicherheitslücken zu schließen. Das bedeutet: Die Hacker können Zugriff auf ihre E-Mails haben. Das Mailsystem ist ein kritischer Punkt für die IT-Sicherheit eines Unternehmens.

- **Ein Spamfilter sortiert eingehende E-Mails vor.**
- **Im Postfach ist eingestellt, dass Bilder nicht automatisch heruntergeladen werden.**

8. Das Team zur »menschlichen Firewall« ausbilden.

Rund 90 Prozent der erfolgreichen IT-Angriffe beginnen mit einer E-Mail. Diese Pishing-Mails kommen z.B. von Kollegen, Geschäftspartnern oder Bewerbern mit der Aufforderung die Mail schnell durchzulesen und zu reagieren. Ziel ist, dass die Mailempfänger die Anhänge schnell öffnen.

Führungskräfte müssen ihrem Team vermitteln, dass kleinsten Unstimmigkeiten im E-Mail-Verkehr Misstrauen wecken sollte. Auch wenn der Absender erst mal vertrauenswürdig aussieht. Mitarbeiter müssen lernen, wachsam zu bleiben.

- **In meinem Unternehmen gibt es regelmäßige Schulungen in IT-Sicherheit.**
- **Mitarbeiter können die Regeln zur IT-Sicherheit jederzeit nachlesen.**

So erkennen Sie Pishing-Mails:

– Schauen Sie, ob die Absenderadresse z.B. Buchstabendreher oder andere minimale Veränderungen eines bekannten Namens aufweist.

– Links nicht einfach anklicken. Fahren Sie mit der Maus über die Verlinkung, dann wird die URL angezeigt, zu der sie führt. Achten Sie besonders auf den Domainnamen (z.B. http://www.meinname.de/). Er sollte zum vermeintlichen Ziel der Verlinkung passen.

– In Word-, Excel- oder Powerpoint-Dokumenten sollten die Markos nicht aktiviert werden. Am besten öffnen Sie diese Dokumententypen gar nicht, wenn Sie von einem unbekannten Absender stammen. Bitten Sie stattdessen um eine PDF-Datei.

– Seien Sie skeptisch, wenn ein Absender Druck aufbaut. Sie sollen sofort etwas ausfüllen oder schnell handeln? Tun Sie lieber nichts.

– Wenn Sie unsicher sicht, googeln Sie die Telefon-Nummer des Absenders und fragen Sie nach, ob er die Mail tatsächlich geschrieben hat. Wählen Sie nicht die Nummer aus der Signatur.

9. Datenverlust mit Back-ups vermeiden

Ein Trojaner hatte den zentralen Server, danach die Computer der Mitarbeiter und das ganze Netzwerk einer Firma infiziert. Trotz dem, dass die Rechner sofort vom Netz genommen und alle Mitarbeiter informiert wurden, war es schon zu spät. Alle Rechner waren infiziert, die Erpresser forderten Bitcoins im Wert von 10.000 EUR. Die Kriminalpolizei gab die Empfehlung kein Lösegeld zu zahlen, da es keine Garantie gebe, dass die Hacker die Dokumente entschlüsseln. Es mussten die ganz IT neu aufbauen: neue Rechner, neue Festplatten, Windows neu installieren.

Aus dieser Erfahrung wurde ein neues Datensicherungskonzept erarbeitet. Anwendungsdaten können bei Bedarf leichter wiederhergestellt werden. Außerdem wurden wichtige Daten wie E-Mail-Archive, Kopien der Datenbanken und Daten aus dem Qualitätsmanagements-Dokumentationssystem auf einen zentralen Back-up Server übertragen und auf Bandlaufwerke gesichert.

- **Machen Sie einen Plan, welche Daten wie häufig gesichert werden müssen.**
- **Testen Sie, ob Ihre Back-ups funktionieren.**

10. Richtlinien für die Qualität von Passwörtern erstellen

Etwa zwei Drittel der Erwachsenen in Deutschland nutzen einer Umfrage zufolge das gleiche Passwort für mehrere Online-Dienste, wie etwa das E-Mail-Postfach, soziale Netzwerke, Banking. Eine gefährliche Bequemlichkeit.

Wer Daten schützen möchte, der braucht ein starkes, sicheres Passwort. In Unternehmen und Organisationen werden zusätzlich neben den Unternehmensdaten auch noch personenbezogene Daten von Betroffenen verarbeitet. Kein Wunder also, dass es gilt diese besonders zu schützen.

Jedes Unternehmen und jede Organisation sollte daher eine Kennwortrichtlinie erstellen, um personenbezogene Daten ausreichend zu schützen. Nicht umsonst stellt diese als technische und organisatorische Maßnahme (TOM) einen wichtigen Bestandteil

zur Einhaltung der DS-GVO (Datenschutzgrundverordnung) dar. Ein nicht ausreichendes Passwort kann unter Umständen sogar zu einem Bußgeld führen.

Checkliste Passwort – Ist mein Passwort sicher?

Passwörter sollten nach gewissen Vorgaben festgelegt werden, damit Sie sicher sind. Unter anderem sollte ein Passwort:

- **mindestens acht Zeichen lang sein**
- **nicht nur Buchstaben beinhalten, sondern aus Groß- und Kleinbuchstaben, Sonderzeichen (Satzzeichen u.Ä.) und Zahlen bestehen**
- **kein sinnbringendes Wort sein, das z.B. im Duden aufgeführt ist**
- **nicht aus einem einfachen Passwort bestehen (z.B. bekannte Namen)**
- **nicht aus Zeichen aufgebaut sein, die auf der Tastatur nebeneinander liegen (z.B. 123456)**
- **mehrfach hintereinander das gleiche Zeichen auf der Tastatur enthalten (z.B. www)**
- **nicht direkt mit dem Benutzer in Verbindung gebracht werden können uvm.**
- **jede Anwendung sollte ein eigenes Passwort haben**

11. Gehen Sie in eine Cloud, die Sie wieder verlassen können.

Achten Sie bei Cloud-Anbietern darauf, wo die Daten liegen und dass sie exportiert werden können.

- **Legen Sie fest, welche Daten in die Cloud sollen.**

12. Ein Plan für den Ernstfall und die Tage danach

- **Bereiten Sie eine Notfallkarte vor, in der steht, was bei einem IT-Notfall zu tun und wer zu informieren ist. Die Informationen müssen regelmäßig aktualisiert werden.**
- **Legen Sie fest, welche Abteilungen nach einem Hacker-Angriff als erste wieder arbeiten können müssen.**

Die inhabergeführte ITeen-Schmiede steht für solide und bezahlbare IT-Dienstleistung – auch bei höchsten Anforderungen! »MADE IN GERMANY!«

Von unserem Hauptsitz in Albstadt und der Niederlassung Trochtelfingen betreuen wir gerne unsere Kunden im süddeutschen Raum.

Alles aus einer Hand!
Clevere IT-Lösungen von der Alb.

Kostenlose Erstberatung!

Jetzt Termin vereinbaren

(0 74 32) 13 097 0

Termin online vereinbaren

www.dieITeenschmiede.de

Die ITeen-Schmiede
Inh. Marco Rukwid
An der Technologiewerkstatt 1
72461 Albstadt
Telefon 0 74 32 – 13 097 0
E-Mail hallo@dieiteenschmiede.de
www.dieiteenschmiede.de