Das Wichtigste im Überblick

IT-Sicherheit 2021

Die schnelle digitale Entwicklung und Veränderung verlangen Unternehmen, Arbeitnehmern und Arbeitgebern einiges ab. Um nicht zu sagen: Sie bringt uns täglich an unsere Grenzen.

Das Problem: Ohne Digital war einmal. Sprich: Ohne geht's nicht mehr. Aber was tun?
Unser Whitepaper zum Thema IT-Sicherheit hilft Risiken zu erkennen und Lücken zu schließen.

Ich wünsche viel Spaß mit mehr Sicherheit!

Ihr Stefan Lanz

Lanz Services GmbH

Stand: 02.08.2021

Paulinenstraße 66, 88046 Friedrichshafen
Fon 07541 - 590 88 88
Mail info@lanz.info

Stefan Lanz
IT-Experte | Digital Native
Berater | Coach

Inhaltsverzeichnis

IT-Sicherheit – Das Wichtigste im Überblick

Cyberkriminalität ist das neue Mekka für Betrüger und Erpresser. Es geht teilweise um Forderungen von bis zu 50 Millionen Euro an gehackte Unternehmen. Regelmäßig erscheinen Berichte über neue Erpressungstrojaner oder Hackerangriffe.

Deshalb spielt die IT-Sicherheit eine größere Rolle denn je. Auch wenn es noch Unternehmer gibt, die das nicht wahrhaben wollen. Vor allem die kleinen und mittelgroßen Betriebe wähnen sich oft sicher, da ein Angriff auf sie vermeintlich nicht so lukrativ ist wie auf große Konzerne. Doch das ist ein Trugschluss. Die Unternehmensgröße spielt für die Cyberkriminellen keine Rolle.

Da diese Art von Kriminalität äußerst lukrativ sein kann, sind die Betrüger sehr erfinderisch, wenn es um neue technische Kniffe geht, mit denen sie die Sicherheitsbarrieren der Unternehmens-IT umgehen können. Daher wird der Kampf zwar schwerer, doch auch die IT-Dienstleister sind nicht auf den Kopf gefallen. Jedes Unternehmen braucht ein individuelles Sicherheitskonzept, um die sensiblen Firmendaten zu schützen. Das Konzept muss regelmäßig von den IT-Sicherheitsexperten angepasst werden.

Dieses Whitepaper fasst für Sie zusammen, welche Sicherheitsrisiken es für die IT in einem Unternehmen überhaupt gibt. Sie erfahren, wie Sie Social Engineering vorbeugen können und worauf Sie bei der Wahl von Passwörtern achten müssen.

Hacker wollen Lösegeld

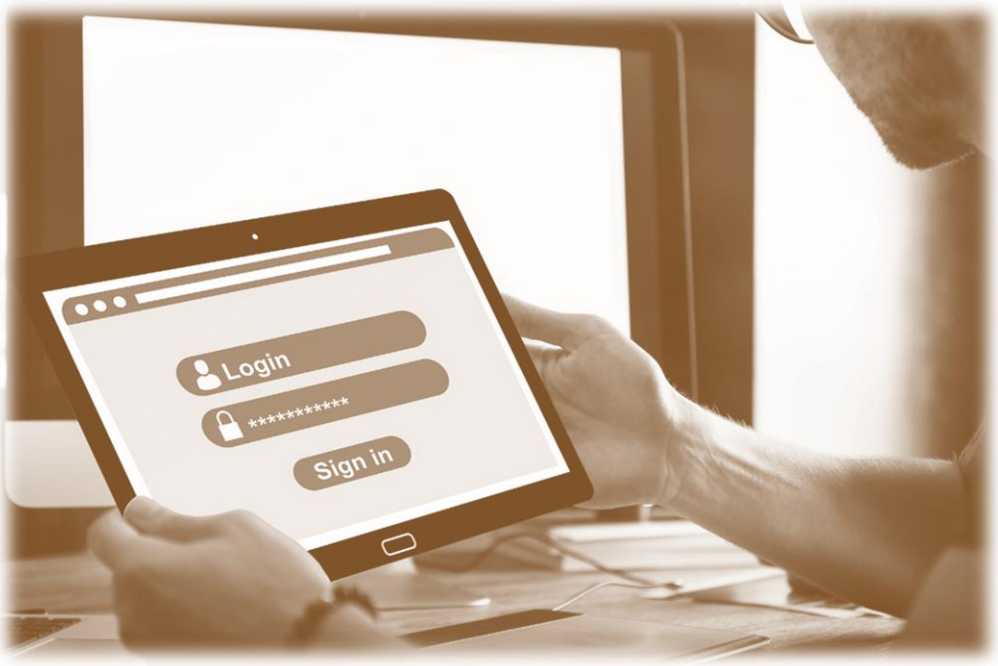
Die sogenannte Ransomware, also Erpressungssoftware, gehört zu den größten Gefahren für die IT-Sicherheit eines Unternehmens. Kriminelle verschlüsseln dabei die Daten auf einer Festplatte oder einem Server, sodass „nichts mehr geht“. Das Arbeiten wird unmöglich gemacht. Erst gegen eine Lösegeldzahlung werden die Daten wieder freigegeben. Dem vorzubeugen, funktioniert mit einer Backup-Strategie. Mit ihr kann man die Daten wiederherstellen. Das ist zwar aufwendig, aber immerhin möglich.

Beliebt ist auch der Datenklau über Phishing-Angriffe. Damit gelangen Hacker an wertvolle Unternehmensdaten, die sie im Darknet verkaufen können. Passwörter und Login-Daten sind besonders begehrt und werden ebenfalls für Angriffe genutzt. Es existieren jedoch bestimmte Lösungsmaßnahmen, die von den IT-Sicherheitsexperten genutzt werden können.

Die Gefahr Social Engineering

Tatsächlich ist das größte Problem laut vielen Studien gar nicht die Technologie, es ist der Mensch, speziell der Mitarbeiter, und zwar zu 60 Prozent. Tendenz steigend. Hier lautet das Stichwort: Social Engineering. Darunter versteht sich die soziale Manipulation – man bringt den Mitarbeiter durch Tricks dazu, etwas am technischen Endgerät (PC, Laptop, Tablet, Smartphone) zu tun, das dem Unternehmen schwer schadet.

Im Grunde werden Mitarbeiter mit Hilfe von falschen Angaben so beeinflusst, dass sie vertrauliche Informationen weitergeben. Damit können die Betrüger Unternehmensdaten, Netzwerk-Passwörter und sogar ganze Firmenkonten lesen. Zu den bekanntesten Vorgehensweisen gehören die Phishing-Mail und der CEO-Betrug. Für so einen Coup spionieren die Kriminellen das persönliche und betriebliche Umfeld ihrer Opfer aus. Sie täuschen häufig Identitäten vor, in dem sie sich beispielsweise als Vorgesetzten ausgeben. In der analogen Welt wären die Social Engineers Hochstapler, im Web gehören sie zu den Cyberkriminellen. Ein Schutz vor ihnen sollte zu jedem IT-Sicherheitskonzept gehören.



Die Methoden der Betrüger

Die beliebtesten Social-Engineering-Methoden sehen so aus:

An erster Stelle steht der vermeintlich vergessene USB-Stick, der plötzlich irgendwo liegt. Der Mitarbeiter prüft ihn an einem Gerät des Unternehmens, doch auf dem Stick befindet sich Schad- oder Spionagesoftware.

Die Phishing-Mail steht genauso weit vorne. Sie bringt den Mitarbeiter dazu, auf einen Link zu klicken oder auf fremden Seiten Kontoinformationen einzugeben. Dieser Methode folgt das Spear-Phishing. Dabei handelt es sich um maßgefertigte Phishing-Mails an einzelne oder kleine Gruppen von Menschen. Tatsächlich wird das Phishing auch per Telefon betrieben, indem die Betrüger beim Mitarbeiter anrufen und sich etwa als Support-Arbeitskraft ausgeben. Auch möglich sind gehackte Webmail-Konten, die als Archiv genutzt werden. Sie behaupten, dass sich zum Beispiel jemand Fremdes am eigenen Google-Konto angemeldet hat und man solle doch bitte prüfen, ob das stimme. Das unerlaubte persönliche Eindringen in ein Bürogebäude kommt an letzter Stelle, wird jedoch nach wie vor von einigen Betrügern umgesetzt.

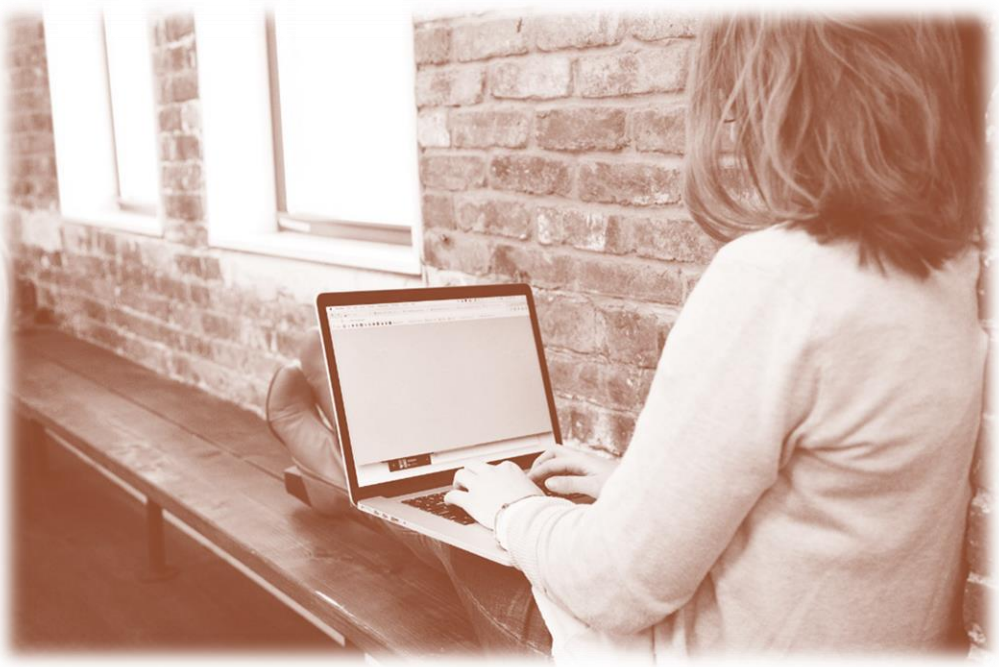
Das können Mitarbeiter tun

Wenn es um den Schutz vor Social Engeneering geht, ist es am wichtigsten, die Mitarbeiter dafür zu sensibilisieren. Sie müssen über die Tricks der Kriminellen umfassend informiert werden und Schulungen zum Thema durchlaufen. Damit gibt die Unternehmensführung ihren Mitarbeitern das Rüstzeug an die Hand, um Social Engeneering überhaupt erst zu entlarven.

Eine Liste mit den wichtigsten Fakten auf einen Blick – wie die Folgende – könnte sich der Mitarbeiter neben den Computer hängen:

- Sensible Daten auf dem PC müssen verschlüsselt sein
- Vertrauliche Informationen dürfen nicht den in sozialen Netzwerken landen
- Auch eigene Daten sollten verantwortungsvoll in sozialen Netzwerken genutzt werden. Dafür muss man regelmäßig die Datenschutzeinstellungen prüfen

- Passwörter, Kontoinformationen oder Zugangsdaten dürfen nicht per E-Mail oder Telefon geteilt werden. Unbekannte Absender, die so etwas fordern, sollten mit großem Misstrauen überprüft werden
- Wer sich auf einer Seite im Internet einloggen will, sollte das genau dort tun und auf keinen Fall über Links aus E-Mails
- In einem Unternehmen müssen feste Richtlinien für den Umgang mit Wechseldatenträgern festgelegt sein. Fremde Datenträger wie USB-Sticks oder CDs stellen ein großes Sicherheitsrisiko dar



Das unterschätzte Passwort

Es wirkt unspektakulär, vielen ist es auch lästig – aber der User kann sich unglaublich viel Ärger ersparen, indem er sich ein sicheres Passwort zulegt. Indem er sich außerdem für jeden Account unterschiedliche Passwörter ausdenkt. Noch immer legen sich viele Deutsche einfach zu merkende und damit auch leicht zu erratende Passwörter an. So gehörten zu den beliebtesten Passwörtern 2018 „hallo 123“, „passwort“ und „123456“.

Schon bei privaten Accounts kann das gefährlich werden, für Unternehmenskonten ist das ein absolutes No-Go. Für Kriminelle wäre das geradezu eine Einladung. Unternehmen müssen die Passwortsicherheit ihren Mitarbeitern daher mindestens im Rahmen von Schulungen näherbringen, besser noch ist die Aufstellung konkreter Regelungen für die Wahl eines sicheren Passworts. Keines ist zu 100 Prozent sicher, das muss dazu gesagt werden. Zweifelsohne aber, kann das Risiko vor Datenklau ganz erheblich verringert werden, etwa, wenn das Passwort regelmäßig gewechselt wird.

Sobald Datenbanken gehackt wurden, sind die gestohlenen Passwörter allerdings schon im Umlauf. Im schlimmsten Fall können Hacker dann frei auf die Daten zugreifen.

Doch wie sieht ein vorbildliches Passwort nun aus?

Grundsätzlich gilt: Es muss mindestens zehn Zeichen umfassen, sollte Sonderzeichen und Zahlen sowie Groß- und Kleinbuchstaben enthalten. Weitere Regeln besagen, dass Passwörter von einer Mehr-Faktor-Authentifizierung begleitet werden sollten. Sie dürfen nie im Klartext abgespeichert werden und sind zudem mit einem anerkannten Verfahren zu hashen. Zuvor sollten sie mit einer zufälligen Zeichenfolge versehen werden, um eine systematische Rückführung von Hashes zu erschweren.

Ein Masterkennwort macht Sinn

Ein Passwortmanager macht für die Verwaltung der Passwörter Sinn. In ihm können sämtliche Passwörter in einer verschlüsselten Datei gespeichert werden. Wer sein Masterkennwort auswendig kennt, kann auf die anderen Passwörter zugreifen. Die meisten Passwortmanager bieten eine Browser-Erweiterung an. In vielen Fällen werden die Eingabefelder auf Login-Seiten dann automatisch mit dem abgespeicherten Kennwort ausgefüllt. Gute Passwortmanager heißen beispielsweise Keeper Security, Lastpass Premium, Dashlane Premium oder Intel Security True Key Premium.

Über viele Passwortmanager lassen sich sogar neue Kennwörter generieren. Sie folgen dabei automatisch den geltenden Sicherheitsregeln. Der User kann auch selbst festlegen welche Zeichen unbedingt enthalten sein sollen. An dieser Stelle überprüft ein guter Manager, ob Nachbesserungsbedarf besteht.

Die Sache mit der DSGVO

Die EU-Datenschutzgrundverordnung (DSGVO) ist nun schon seit 2018 aktiv. Dennoch hatten kurz vor der Deadline damals nur 32 Prozent der Unternehmen die Anforderungen des Gesetzes größtenteils umgesetzt. Unsicherheit herrscht vielerorts sogar heute noch, obwohl die Unternehmen gut daran täten, auf der rechtssicheren Seite zu sein.

Der Datenschutz war zuvor durch das Bundesdatenschutzgesetz geregelt, die DSGVO geht in einigen Passagen darüber hinaus. Vor allem sind personenbezogene Daten schon dann verletzt, wenn sie deren Verfügbarkeit nicht gewährleisten können. Dokumentationspflichten sowie Betroffenenrechte wurden ausgeweitet und Bußgelder deutlich erhöht. Es können nun Strafen von bis zu 20 Millionen Euro - also vier Prozent des weltweiten Umsatzes des betroffenen Unternehmens - erhoben werden.

Auf diese Fragen kommt es an

Gehen personenbezogene Daten abhanden, sind die finanziellen Schäden für Unternehmen sehr hoch. Je nach Umfang betragen die Kosten für ein Datenleck rund 3,9 Millionen Euro (Stand 2018). Darin enthalten sind die Kosten für die Arbeitsstunden, die Unternehmen zur Reparatur der Datenpanne aufwenden müssen, die Wiederherstellung der Daten und die hohen Bußgelder. Die DSGVO hat nichts daran geändert, dass das Risiko weiter steigt, Opfer eines Cyberangriffs zu werden. Im Gegenteil – um auf der sicheren Seite zu sein, ist viel Arbeit nötig. Diese Fragen sollten im Rahmen der Verordnung geklärt sein:

- Wer ist für die Einhaltung der DSGVO verantwortlich?
- Ist die IT-Struktur ermittelt und dokumentiert (inklusive mobile Endgeräte)?
- Ist die IT widerstandsfähig gegen Systemausfälle und Cyberangriffe aufgestellt?
- Wurde die Verschlüsselung von Daten verbessert?
- Wurden mögliche Kosten eines mangelhaften Datenschutzes bewertet und abgewogen? Möglicherweise muss das Unternehmen hier sein Budget anpassen.
- Wurde das Recht auf Vergessen, also ein Löschkonzept, umgesetzt?
- Ist die Geschäftsleitung darüber informiert worden, welche Bußgelder bei Nicht-Umsetzung der DSGVO erhoben werden können?
- Ist die Technik auf dem neuesten Stand, sodass sie das Risiko eines Angriffs minimieren kann?
- Gibt es einen Datenschutzbeauftragten?
- Gibt es ein aktuelles Verarbeitungsverzeichnis?
- Ist die Datenstruktur dokumentiert und gibt es einen Überblick darüber, wo sich welche Kundendaten befinden?
- Sind die Verträge in Sachen Auftragsverarbeitung angepasst worden?
- Wurden Datenschutzmaßnahmen ergriffen und deren Umsetzung dokumentiert sowie kontrolliert? Bei einer Prüfung durch Aufsichtsbehörden ist das wichtig.
- Sind interne Kontrollprozesse und technische sowie organisatorische Prozesse eingerichtet worden?

Sicherheitstrends erkennen

WannaCry und Petya sind nur zwei der Cyberangriffe, die in den vergangenen Jahren für Aufruhr sorgten. Und: Die nächsten Übergriffe kommen sicher. Cybersicherheit ist und bleibt für Unternehmen eine große Herausforderung, je mehr das tägliche Leben durch Vernetzung bestimmt ist. Im privaten Bereich ist das Smart-Home ein Thema, in der Industrie tun sich stetig mehr Sicherheitslücken durch Automatisierung und Industrie auf.

Dass sich die Hacker-Angriffe immer wieder wandeln, ist das größte Problem. Kriminelle greifen gezielter an und ändern ihre Angriffsziele, beispielsweise im Gesundheits- oder Energiesektor. Derzeit gehören das Internet of Things genauso zu den Cybersicherheitstrends wie Industrial Internet, künstliche Intelligenz, Zertifizierungen oder biometrische Authentifizierung. Nicht zu vergessen sind die neuen Konzepte, um Bedrohungen zu erkennen.

Diese Regeln sollten erfüllt sein

Die Bedrohungen durch die Cyberkriminellen ändern sich, die Maschen bleiben jedoch gleich. Phishing und Datenklau sind wie gesagt die beliebtesten Angriffsmethoden durch die Betrüger: damals wie heute. Die Angriffsweise hat sich aber gewandelt, denn es kommen stetig neue Technologien zum Einsatz. Bei Ransomware-Angriffen etwa, nehmen die Hacker gezielt einzelne Unternehmen ins Visier. Bislang ging es dabei nur um groß angelegte Lösegeldforderungen. Es lohnt sich also für Unternehmen, noch mehr in die IT-Sicherheit zu investieren. Die gute Nachricht: Mehr Unternehmen als je zuvor sind sich bewusst darüber, wie grundlegend wichtig IT-Sicherheit ist.

Es gibt einige Punkte, hinter die ein Unternehmen in Sachen IT-Sicherheit seinen Haken setzen sollte. Vor allem hier:

- Die aktuellen Sicherheitsupdates befinden sich auf den Betriebssystemen.
- Es existiert ein Notfallplan, sollte es einen Cyberangriff oder eine Datenpanne geben. Damit ist klar, was bis wann und in welchem Umfang wieder hergestellt sein muss.
- Das Unternehmen nutzt ein regelmäßig aktualisiertes Virenschutzprogramm und eine Firewall zum direkten Schutz vor Hackerangriffen von außen.
- Die Server und Clients (PCs) sind tagesaktuell mit Sicherheitsupdates versorgt.

- Eine Datensicherung (mindestens 2 Methoden mit 2 unterschiedlichen Medien) ist eingerichtet.
- Die Datensicherung wird regelmäßig kontrolliert und auf Wiederherstellbarkeit getestet.
- Die Mitarbeiter sind aktuell zu den Themen Phishing, Spam und Social Engineering geschult und werden regelmäßig auf ihr Wissen hin getestet.
- Administratorrechte besitzen nur die Mitarbeiter, die sie zwingend benötigen
- Alle Vorgaben zur DSGVO sind umgesetzt und werden laufend kontrolliert und weiterentwickelt.

Über Stefan Lanz & Lanz Services GmbH

Stefan Lanz (*1977) ist verheiratet und hat 2 Kinder.

Er berät seit mehr als 25 Jahren Unternehmen im Bereich Informations- und Kommunikationstechnik.

Er ist zudem IT-Sachverständiger, IT-Sicherheits- und Datenschutzbeauftragter, hat eine Coaching-, Moderatoren- und Trainer-Ausbildung mit zertifiziertem Abschluss.

Seit dem 6 Lebensjahr sitzt er selbst am PC und hat die Höhen und Tiefen digitaler Entwicklung hautnah miterlebt.

Als Unternehmer seit dem 18. Lebensjahr hat er Erfahrungen in nahezu allen Bereichen der IT- und Kommunikationstechnik und rund um das Internet gesammelt.

Als Sohn zweier Lehrer bestimmte außerdem das „angeborene" Lehrergen und die damit einhergehende „Liebe für die Menschen" sein Leben.
So engagierte er sich bereits in Jugendjahren als Gruppenleiter in Vereinen und bei der kath. Kirche und hält seither regelmäßig Vorträge, gibt Workshops und Seminare und begleitet Menschen rund um ihre Entwicklung in dieser schnelllebigen Zeit.

Sein Motto

Probleme kann man nicht mit derselben Denkweise lösen, mit der sie entstanden sind.
(Albert Einstein zugeschrieben)

Sein Anliegen

Menschen und Unternehmen dabei zu unterstützen, Fortschritte zu machen, Weiterzukommen, sich zu ent-wickeln und zu wachsen.

Sein Ansporn

Das Leben ist Veränderung – nicht nur heute und morgen, sondern jeden neuen Tag. Diese Veränderung bietet laufend neue Chancen für jede und jeden von uns. Wir müssen Sie nur ergreifen.

Weitere Infos zu Stefan Lanz finden Sie unter http://stefan.lanz.info

Man muss nur wollen

und daran glauben,

dann wird es gelingen.

(Ferdinand Graf von Zeppelin)