eBook:

Computer- & Netzwerksicherheit für Unternehmen

Davor müssen Sie sich 2017 schützen!

4 aktuelle IT-Sicherheitsbedrohungen leicht verständlich erklärt

Inhaltsverzeichnis

Vorwort

In diesem eBook erklären wir Ihnen leicht verständlich, welche IT-Bedrohung auf österreichische Unternehmen im Jahr 2017 zukommen.

Die Bedrohungsszenarien durch Cyberkriminalität sind hierzulande längst Realität. Verantwortungsvolle Unternehmer müssen hier vorsorgen. Mehr als 10.000 angezeigte Fälle beim österreichischen Bundesministerium für Inneres pro Jahr machen dies deutlich. Österreich ist kein blinder Fleck in den Augen der Hacker. Diese wirtschaftliche Bedrohung ist global und flächendeckend.

Es geht uns hier vor allem um Situationen, die uns tatsächlich konkret **in Österreich** betreffen. Die beschriebenen Situationen **sind direkt** aus unserem **Kunden „Alltag“** gegriffen und nicht fiktiv von einem Security-Hersteller, der Ihnen Angst machen möchte!

Zusätzlich geben wir Ihnen, sofern möglich, kurze und nachvollziehbare Tipps wie Sie sich vor den wichtigsten Bedrohungen schützen können. Und zwar meist ohne, dass Sie sich irgendeine teure Software anschaffen müssen. Im Detail stehen Ihnen natürlich unsere Security-Experten gerne mit Rat und Tat zur Seite.

Möchten Sie mehr über mich als Autor dieses eBooks bzw. über mein Unternehmen erfahren, besuchen Sie uns am besten auf unserer Website unter…

https://www.rysit.at/

Und nun viel Spaß beim Lesen des aktuellen eBooks!

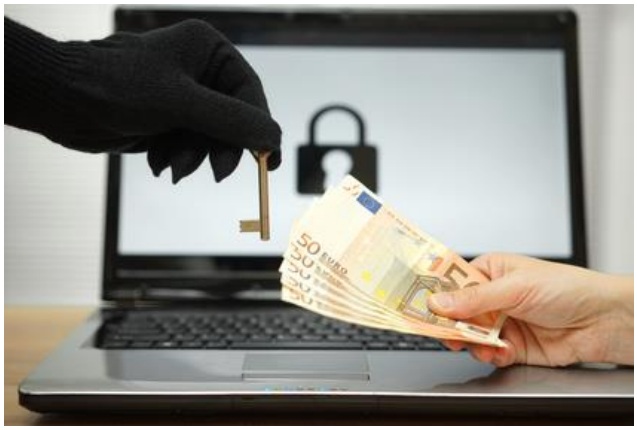
Mit herzlichen Grüßen,

Richard Schranz

Geschäftsführer und Eigentümer

RYSIT Consulting GmbH

Thema 1: Kryptotrojaner



10.010 Fälle von Cyber-Kriminalität registrierte das österreichische Bundeskriminalamt im Cybercrime-Report 2015 (derzeit der aktuellste). **Kleine und mittlere Betriebe standen bisher im Fokus.** Die Angriffe auf große Betriebe steigen an. Doch Unternehmen – egal ob klein oder groß – sind dem nicht schutzlos ausgeliefert, wir zeigen Ihnen, wie Sie es Angreifern so schwer wie möglich machen.

Was ist ein Kryptotrojaner?

Die Kryptotrojaner werden auch Verschlüsselungstrojaner, Erpressungstrojaner oder Ransomware genannt. Im Jahr 2016 wurden sie zur **größten Cyber-Kriminalitäts-Bedrohung für Unternehmer im deutschsprachigen Raum**. Auch für das Jahr 2017 wird den Kryptotrojanern vorausgesagt, dass diese die meisten Schäden anrichten werden.

Es handelt es sich dabei um Schadsoftware, die sich auf einem oder mehreren Geräten in Ihrer Firma einnistet. Computer fangen sich diesen schädlichen Trojaner meist über infizierte E-Mail-Anhänge oder ungesicherte Internetbrowser ein.

Innerhalb kürzester Zeit nach der Infizierung sind **Ihr ganzer Computer und/oder einzelne Teile nicht mehr einsetzbar.** Lässt man den Virus ungehindert walten, verteilt sich dieser zusätzlich auf Ihr **komplettes Firmennetzwerk**, befällt andere PC oder noch schlimmer, **das zentrale Speichersystem**. Daten, die darauf gespeichert sind, werden verschlüsselt. Sie können nicht mehr darauf zugreifen.

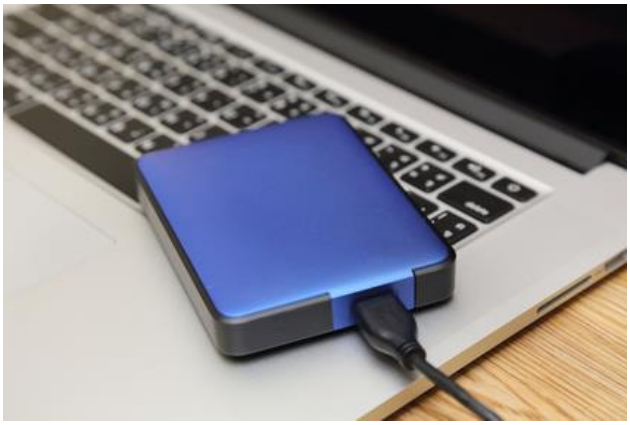
Die Masche der Angreifer: Wenn Sie einen gewissen Geldbetrag überweisen, bekommen Sie einen Schlüssel zugesandt. Wenn Sie diesen eingeben, können Sie Ihren PC wieder wie gewohnt verwenden. Sie müssen praktisch „**Lösegeld**“ für Ihren eigenen Computer / Ihr eigenes Netzwerk bezahlen.

Harmlosere Varianten des Kryptotrojaners sperren nicht den ganzen Computer oder ganze Ordner, sondern lösen nur immer wieder lästige Pop-Ups aus. Die Lösung, die Ihnen die Hacker bieten, ist aber immer die Gleiche.

Ihr Problem: Selbst wenn Sie bereit sein sollten, das „Lösegeld“ für Ihre Daten zu bezahlen, gibt es keine Garantie für Sie. Niemand garantiert Ihnen, dass die Angreifer die Schadsoftware wirklich entfernen. Niemand garantiert Ihnen, dass die Schadsoftware nicht wieder aktiviert wird. Daher empfiehlt das Bundeskriminalamt auch ganz klar, dass Sie kein Geld an die Erpresser zahlen sollten.

Wie können Sie Ihr Unternehmen schützen?

Gleich vorweg: Es gibt keinen ultimativen Schutz gegen Hacking-Angriffe. Sie können es den Angreifern allerdings so schwer wie möglich machen. Zudem können Sie eine Sicherheitsvariante einbauen, die vor allem Ihren Schaden IMMER auf ein Minimum senkt:



- **Backups, Backups, Backups:** Das ist genau jene Sicherheitsmaßnahme mit der Sie das Risiko stets niedrig halten können. Wenn Sie jederzeit dazu in der Lage sind, den Zustand Ihres Computers vor der Infizierung wiederherzustellen, dann haben Sie den Schaden so gering wie möglich gehalten. Meist ist dann auch kaum ein Schaden entstanden, da die Verschlüsselung meist sehr kurz nach der Infizierung auftritt.
  Wenn Sie innerhalb von wenigen Stunden Ihr Backup wieder einspielen, haben Sie auch nur diese Stunden an Arbeit verloren und können komplett sorgenfrei weiterarbeiten. Ein Backup schützt Ihr System übrigens nebenher nicht nur gegen Angriffe von außen, sondern auch vor Eigenfehlern. Sollten Sie eine Datei irrtümlich vernichten, diese aber später doch wieder brauchen, steht sie Ihnen aufgrund des Backups auch wieder zur Verfügung.

- **Aktuelle Virenschutz-Software:** Selbst die beste Virenschutz-Software ist den Hackern immer einen Schritt hinten nach. Aber: Je aktueller Ihre Schutzsoftware ist, desto mehr Bedrohungen kann sie verhindern. Denn die Entwickler der großen Virenscanner arbeiten Tag und Nacht daran, Ihren Schutz zu verbessern. Sobald es eine neue Bedrohung gibt, wird eine Aktualisierung des Virenscanners vorgenommen. Diese greift aber natürlich nur, wenn Sie diese auch auf Ihrem Computer installieren.
  Beim Einsatz von Virenschutz-Software gilt: Setzen Sie diese für alle Clients, für alle Datenserver, den Webzugriff und E-Mail-Transfers auf!

- **Firewall:** Eine Firewall, die Ihr Firmennetzwerk vor unbefugten Netzzugriffen schützt, ist essentiell. Wie beim Anti-Virenprogramm gilt, dass es keinen absoluten Schutz gibt. Aber eine gute Firewall macht es jedem Angreifer deutlich schwieriger. Und nur die besten Hacker beißen sich an einer solchen nicht die sprichwörtlichen Zähne aus.

Thema 2: Hacking von Telefonanlagen

Das Bundesministerium für Inneres (BMI) warnt: **Immer mehr österreichische Unternehmen werden Opfer des Hacking von Telefonanlagen.** Dadurch entstehen schwere Schäden. Auch die CFCA, ein internationales Institut zur Verhinderung von Betrugsfällen, berichtet: Jedes Jahr entsteht deshalb weltweit ein Schaden von etwa 4,1 Milliarden Euro. Hier erfahren Sie was Hacking von Telefonanlagen ist und wie Sie sich davor schützen können.

Was ist Hacking von Telefonanlagen?

Hacking von Telefonanlagen wird im Fachjargon auch Phreaking genannt (eine Mischung aus den englischen Begriffen „phone“ und „freak“). Ursprünglich wurde dieser Begriff in den 60er Jahren verwendet. Mittels eines Signals in der Frequenz, die auch vom Telefonanbieter verwendet wurde, konnte man gratis telefonieren.

Diese Praxis ist bereits lange ausgestorben, aber das moderne Internet bietet Hackern eine neue Angriffsmöglichkeit. Im geschäftlichen Alltag bieten VoIP-Telefone klare Vorteile gegenüber klassischer Telefonanlagen. Die neuen Funktionen haben auch das Interesse von Betrügern geweckt.

Hacker verschaffen sich Zugang zu ungeschützten Telefonanlagen, um außerhalb der Geschäftszeiten bei vorher eingerichteten Mehrwert- oder Auslandsnummern anzurufen.

So machen Hacker den Schaden immer größer

Sind Hacker erfolgreich wächst der Schaden sehr schnell. Ein **wahrer Schneeballeffekt** wird losgetreten: Die Zugänge zu den Telefonanlagen werden unter den Hackern verteilt. Innerhalb kürzester Zeit entstehen Schäden im fünfstelligen Euro Bereich.

Eine australische Firma erlitt so sogar Schäden von mehr als 90.000€. Ihre Telefonanlage wurde gehackt und die Zugangsdaten weltweit verteilt. Innerhalb weniger Monate musste der Betrieb Konkurs anmelden.

Wie die Warnung des BMI zeigt, lebt man auch in Österreich diesbezüglich nicht auf einer geschützten Insel. **Für das Eindringen in Telefonanlagen genügt bereits geringes technisches Know-how.** Das Schlimme an der Sache: Bis der Angriff erkannt wurde, hat man meist die erste hohe Telefonrechnung in der Hand. Die Kosten müssen auch vom Unternehmen getragen werden, da es praktisch unmöglich ist die Schuldigen ausfindig zu machen.

Wie können Sie ihr Unternehmen schützen?

Am wichtigsten ist hierbei vorbeugende Maßnahmen zu treffen. Ist jemand erst einmal ins System eingedrungen, so fällt es schwer dies sofort zu bemerken. Zudem **reicht bereits ein Tag, um erhebliche Schäden anzurichten.**

Ein absoluter Schutz gegen Phreaking existiert nicht. Mit diesen Maßnahmen machen Sie es den Hackern aber schwerer und sie suchen sich vermutlich ein leichteres Opfer:

- **Keine werkseitigen Passwörter:** Sollten Sie noch nie das Passwort verändert haben, ist immer noch das Standardpasswort in Verwendung. Ändern Sie dieses bitte sofort! Hacker wissen von jedem Hersteller darüber Bescheid. Überlegen Sie sich starke Passwörter (Sonderzeichen, Zahlen, Groß- und Kleinschreibung, ausreichende Länge) und erneuern Sie Ihre Passwörter regelmäßig (min. 2x pro Jahr). Besonders bei den Passwörtern für Fernwartungszugänge müssen Sie aufpassen.

- **Extra-Passwörter für bestimmte Funktionen:** Setzen Sie ein Passwort, um Ferngespräche oder Gespräche mit Premium-Rufnummern führen zu können.

- **Schutz gegen Weiterleitungen:** Richten Sie auch einen Schutz gegen externe Weiterleitungen ein. Zudem können Sie noch ausgehende Anrufe außerhalb der Geschäftszeiten sperren lassen.

- **Immer neueste Software:** Überprüfen Sie ob Ihre Software auf dem neuesten Stand ist. Gehen Sie sicher, dass alle nötigen Sicherheitsupdates und Patches installiert sind. Ansonsten können Hacker über bereits bekannte Sicherheitslücken leichter ins System eindringen. Mittels Aktualisierungen werden diese Sicherheitslücken ausgebessert. Neue Schwachstellen müssen dann erst gefunden werden.

- **Mitarbeiterschulung:** Informieren Sie Ihre Mitarbeiter über das Risiko. Diesen können ungewöhnliche Anrufe auffallen und Ihnen melden. Erinnern Sie sie daran, keine technischen Details der Kommunikationssysteme weiter zu geben.

- **Starke IT-Partner:** Setzen Sie Maßnahmen zusammen mit Ihrer IT-Support-Firma. Diese kann Sie warnen, falls ungewöhnlich viele oder teure Gespräche geführt werden. Somit wird der Schaden minimiert und Sie können weitere Schritte einleiten.

Thema 3: Gezielter Diebstahl von mobilen Endgeräten

Diebstahl von Handys, Tablets oder Notebooks ist ein Problem für Unternehmen. Sogar dann, wenn Mitarbeiter für die Arbeit eigene Geräte verwenden. Viele Firmen kennen das Risiko gar nicht.

Wieso ist der Diebstahl von mobilen Endgeräten für Firmen so gefährlich?

23 % aller Österreicher besitzen ein Firmenhandy. Aufgrund des Bring-Your-Own-Device (=“Nimm dein eigenes Gerät“) Trends, werden nun sogar Privathandys vermehrt für Firmenzwecke verwendet. Auf diesen befinden sich dann auch automatisch Daten und Nummern der Firma.

Die Gefahr eines Diebstahles ist allgegenwärtig: **Alle 15 Minuten wird ein Handy in Österreich gestohlen.** Somit sind Handys das Hauptziel von Diebstählen bei mobilen Endgeräten. Aber auch Tablets und Notebooks werden immer häufiger gestohlen. Die Aufklärungsrate liegt laut Polizei bei nur 6%.

Was kann passieren?

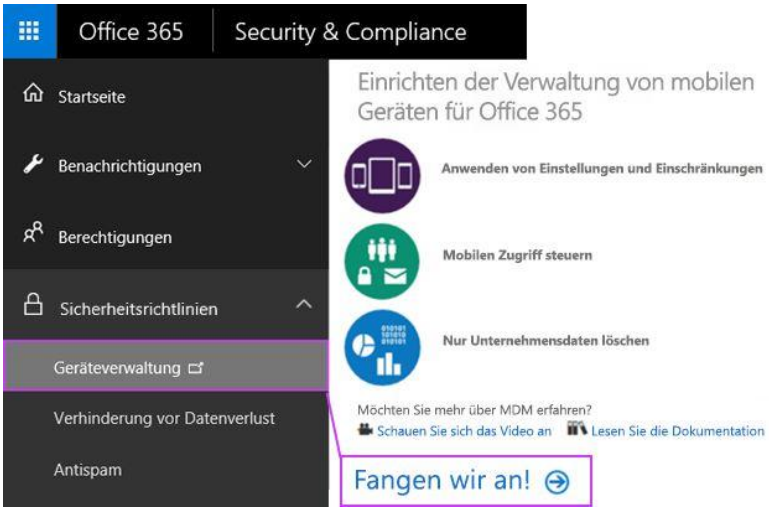
Zusammen mit dem gestohlenen Gerät sind alle gespeicherten Firmendaten in anderen Händen. Im besten Fall gehen Ihnen wichtige Daten und Kundenkontakte lediglich verloren. **Verwenden jedoch Diebe die gespeicherten Daten, geraten Sie sehr schnell in eine missliche Lage**.

Die Situation beginnt beim Missbrauch von Kundenkontakten durch falsche E-Mails oder Anrufe. Das Schlimme ist, diese wirken auf Ihre Kunden seriös, da Sie ja von Ihnen zu kommen scheinen. Somit werden diese Kontaktaufnahmen als vertrauenswürdig eingestuft.

Zudem könnten Unternehmensgeheimnisse an die Konkurrenz gelangen. Oder heikle Anmeldedaten wie Bankzugänge geraten in die falschen Hände.

Wie können Sie sich weitestgehend schützen?

Das Zauberwort heißt: Mobile Device Management (MDM). Das bedeutet „Verwaltungssystem für mobile Endgeräte“. Daten auf firmeneigenen und privaten mobilen Endgeräten können damit geschützt werden.



Dies stellt für Unternehmen aber oft eine große Herausforderung dar. Vor allem auf privaten Geräten Kontrolle und Transparenz zu schaffen, ist eine schwierige Angelegenheit. Durch MDM ist es Ihnen aber möglich, sowohl private als auch firmeneigene Handys, Tablets und Laptops einheitlich zu verwalten.

Neue Geräte können dadurch zentral angemeldet und konfiguriert werden. Selbst Geräte verschiedener Betriebssysteme lassen sich zentral organisieren.

Maßnahme 1: Per Fernbedienung das Geräte sperren oder Daten löschen

Sie können über das MDM-System zentral Änderungen an allen registrierten Geräten vornehmen. Dies ermöglicht Aktionen wie Zurücksetzen des Kennworts oder Sperren des Gerätes. Über die Verwaltung können alle Unternehmensdaten- und Anwendungen im Falle eines Diebstahls gelöscht werden.

Auch Apps lassen sich zentral von einer Stelle aus verwalten. Diese können von Ihnen konfiguriert und zugleich aktualisiert werden. Somit entscheiden Sie, wie die Unternehmensdaten in mobilen Apps verwendet und freigegeben werden.

Daten einzelner Apps lassen sich auch wieder löschen. Sogar das Nutzungsverhalten von Mitarbeitern lässt sich kontrollieren.

Zudem können noch weitere Einschränkungen auf den Browser angewendet werden. Spezifische Websites können so entweder freigegeben oder gesperrt werden.

Weitere Funktionen, die dank MDM Ihre Sicherheit erhöhen:

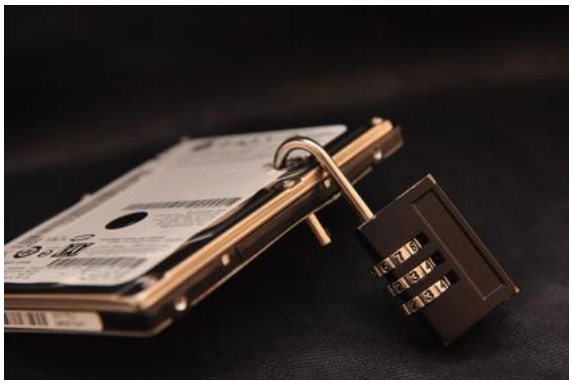
- Bestimmte Funktionen nur mit Kennwort verfügbar machen
- Festlegen wie lange oder wie oft Kennwörter gültig sind
- Anzahl erlaubter Anmeldeversuche reduzieren
- Gewisse Funktionen grundlegend sperren, z.B. Kamera

Maßnahme 2: Statten Sie Ihre Daten mit einem „Reisepass“ aus

Schutz sensibler Zugangsdaten wie Passwörter zu Wlan-Profilen, E-Mails und VPN-Profilen wird durch Zertifikate ermöglicht. Das Zertifikat erfüllt die gleiche Funktion wie Ihr Reisepass. Es weist ganz klar aus, um welches Gerät es sich handelt.

Das Unternehmen verschlüsselt und versendet sensible Daten. Registrierten Geräten wird sozusagen ein Schlüssel zugewiesen. Dieser Schlüssel wird verwendet, um die verschlüsselten Daten lesen zu können.

Gerät nun ein mobiles Endgerät in die Hände von Dieben, so finden diese nur verschlüsselte Daten vor. Die einzige Möglichkeit Zugang zu den Daten zu erhalten, ist diesen Schlüssel zu knacken. Aber bis dahin haben Sie bereits über die Verwaltung die Unternehmensdaten gelöscht.



Für Laptops stehen noch weitere Optionen zur Verfügung

- Aktualisierungen der Software verwalten: Sie entscheiden wann Updates angewendet werden und halten alle Notebooks und PCs auf neuestem Stand.
- Firewall-Richtlinien setzen: So stellen Sie sicher, dass die Firewall auf allen Geräten ordnungsgemäß eingerichtet und eingeschaltet ist.
- Verwaltung von Softwarelizenzen: Informationen darüber, welche Lizenzen wie lange noch verwendbar sind und wie viele noch verfügbar sind und weitere Funktionen.

Durch ein MDM schützen Sie nicht nur Ihre Daten. Sie erlauben es Mitarbeitern auch von jedem Ort aus gefahrlos und produktiv zu arbeiten. Sie können somit einheitlich auf benötigte Unternehmensdaten auch von privaten Geräten zugreifen. Das Risiko für das Unternehmen bleibt jedoch gering.

Eine Vielzahl von MDM-Systemen stehen auf dem Markt zur Auswahl. Wir empfehlen Ihnen die Verwendung von Microsoft Intune zur Sicherung aller Ihrer Geräte. Intune bietet alle vorher genannten Funktionen (und noch mehr), die für Ihren Schutz notwendig sind.

Die ersten Schritte können Sie sicherlich mit der Hilfestellung der Microsoft-Support-Seite selbst bewältigen. Ohne das nötige Know-how werden Feinheiten jedoch schwer umsetzbar sein. Sollten Sie Unterstützung oder eine umfassende Sicherheitsstrategie benötigen, stehen wir Ihnen jederzeit zur Seite.

Teil 4: Intelligente Hacking-Angriffe

Intelligente Hacking-Angriffe verschaffen sich gezielt Zugriff zu Ihrem Unternehmens-netzwerk und nisten sich dort ein. **Die Hacker wissen im Vorhinein, wo sich sensible Daten in Ihrem Unternehmen befinden** und wie sie diese gegen Sie verwenden**.**

Wie unterscheiden sich diese Angriffe von herkömmlichen Hacking-Angriffen?

Herkömmliche Hacking-Angriffe auf ein Unternehmen sind zumeist nicht zielorientiert. Hierbei gilt es, den leichtesten Opfern so viel Schaden wie möglich anzurichten. Um wen es sich dabei handelt, spielt keine Rolle.

Zudem wird nur über kurze Zeit auf das Unternehmensnetzwerk zugegriffen. Man versucht so schnell wie möglich in das Netzwerk einzudringen und es auch wieder zu verlassen. Erwischt wollen die Hacker ja auf keinen Fall werden.

Die Diebe wissen nicht, was für eine Art von Daten sie vorfinden, noch wo sie danach suchen müssen. Somit werden auch weniger Daten gestohlen. Zudem stehen sie unter Zeitdruck, nicht vom Sicherheitssystem entdeckt zu werden.

Um möglichst viel Schaden in kurzer Zeit zu verursachen, greifen diese dann oft zu Schadsoftware, die auf den Rechnern installiert wird. Lesen Sie mehr darüber in dem ersten Teil der Serie.

Was genau sind nun intelligente Hacking-Angriffe?

Intelligente Hacking-Angriffe werden in der Fachsprache „Advanced Persistant Threads“ (APT) genannt. Das bedeutet so viel wie „fortgeschrittene, andauernde Bedrohung“. „Andauernde Bedrohung“, weil sich Hacker über lange Zeit hinweg in

Ihrem System aufhalten. Um nicht von einem Sicherheitssystem entdeckt zu werden, schreiben diese ständig den Code um. Daher „Fortgeschritten“, weil beträchtliches Know-how für solche Aktionen notwendig ist.

Solche Angriffe verzichten auf den Einsatz von Schadsoftware im herkömmlichen Sinn. Schaden will man an dem System keinen anrichten, sondern über Programme heimlich Informationen speichern. Denn man will über einen langen Zeitraum möglichst unbemerkt bleiben. Ein Schaden am System würde sofort bemerkt werden.

Somit bleibt genug Zeit, alle Daten zu entziehen, zu analysieren und dann mit einem ausgeklügeltem Plan vorzugehen. **Der Fokus liegt nur darauf, Ihrem Unternehmen sensible Informationen zu entziehen und Ihnen mit diesen Informationen zu schaden.**

Wie funktioniert ein APT-Angriff?

Phase 1: Erster Zugriff auf das System

Den ersten Zugriff auf das Netzwerk erlangen Hacker über mehrere Methoden. Die Bekannteste ist das Eindringen in das System über eine Sicherheitsschwachstelle. Oft werden auch E-Mails mit schädlichem Anhang an Mitarbeiter versendet. Öffnen diese den Anhang, so kann über das schädliche Programm auf das System zugegriffen werden.

Eine weitere Methode wird „Spear-Phishing“ genannt. Mithilfe von betrügerischen E-Mails, werden Mitarbeiter auf falsche, aber echt wirkende Websites weitergeleitet. Dadurch können Zugangsdaten der Mitarbeiter erlangt werden. Ein E-Mail Account der Firma genügt den Hackern bereits, um in das System einzudringen.

Phase 2: Langfristige Spionage gewährleisten

Nachdem der Zugriff auf das Unternehmensnetzwerk gesichert ist, wird eine Hintertür erstellt. Diese Hintertür dient dazu, dass der Hacker immer auf das System zugreifen kann. Selbst wenn Sie die Zugangsdaten ändern. Eine Vielzahl solcher Hintertüren wird im Verlauf des Angriffs erstellt, um sicher zu gehen, auf alle Teile des Systems zugreifen zu können.

Jetzt gilt es für möglichst lange Zeit nicht entdeckt zu werden, während das System ausspioniert wird. Das Sicherheitssystem Ihrer Firma wird genau auf zusätzliche Schwachstellen untersucht. Zudem wird ausfindig gemacht, wo genau sich sensible Informationen befinden. Danach wird ein Plan entwickelt, wie man möglichst unbemerkt durch diese Schwachstellen auf die sensiblen Informationen zugreifen kann.

Phase 3: Sammeln von Daten

Nun wird der Plan umgesetzt. Auf sensible Informationen wird über lange Zeit zugegriffen und alle Daten werden aufgezeichnet. Zusätzlich werden oft Programme installiert, die im Hintergrund Daten sammeln.

Es kann z.B. ein interner Mitarbeiter-Bereich so umprogrammiert werden, dass bei Eingabe sämtlicher Passwörter diese auch heimlich gespeichert werden. Während dieser Phase befinden sich alle Informationen noch innerhalb der Firma.

Phase 4: Extrahieren der Daten

Sind erst alle nötigen Daten vorhanden, werden diese gespeicherten Informationen nun aus dem Unternehmen gezogen. Gibt es einen Auftraggeber, werden die Daten an diesen weitergeleitet.

Andernfalls schließen sich meistens mehrere Hacker in ein Team zusammen und analysieren genau, wie sie mit den Daten so viel Geld wie möglich für sich rausholen können – natürlich auf Kosten Ihres Unternehmens.

Beispielsweise können Sie aus Ihrem eigenen Unternehmen „ausgesperrt“ werden. Ohne Zahlung eines Lösegelds können Sie auf das eigene System nicht mehr zugreifen.

Wie kann man sich davor schützen?

Leider handelt es sich hierbei um sehr komplexe Angriffe, welche es auf das ganze Unternehmensnetzwerk abgesehen haben. Einfache Maßnahmen, um diese zu verhindern, gibt es leider nicht. Die beste Chance so einen Angriff zu erkennen, erfolgt über Ihren System-Administrator. Dieser kann ungewöhnliche ausgehende Daten der Firma erkennen. Wenden Sie sich daher an diesen.

Wir stehen Ihnen natürlich als Ansprechpartner jederzeit zur Verfügung. Zusammen können wir Maßnahmen setzen, um das Risiko so gering wie möglich zu halten.

Intelligente Hacking-Angriffe setzen sich nur sensible Unternehmensdaten als Ziel. Um diese zu bekommen, verbringen die Hacker längere Zeit in Ihrem Unternehmensnetzwerk. Mittels eines detaillierten Plans gehen diese dann vor und stehlen alle Informationen, die sie zu Ihrem Nachteil nutzen können.

Sie als Unternehmer/Mitarbeiter bemerken den Angriff oft erst, wenn er schon lange vorbei ist. Zugangsdaten funktionieren nicht mehr und plötzlich besitzen Konkurrenten Informationen, die sie auf keinen Fall wissen sollten. Die Komplexität ist leider so hoch, dass einfache Maßnahmen nicht mehr dagegen ankämpfen können.

Fazit:

Als Unternehmer sind Sie solchen Angriffen nicht schutzlos ausgeliefert. Wie Sie sehen, können Sie einige der genannten Maßnahmen vermutlich schon alleine – also ohne IT-Techniker – umsetzen. Jede kleinste Verbesserung kann für sich genommen schon einen Angriff abwehren. Sie können Ihre Sicherheitsposition also nur stärken.

Falls Sie doch einmal Unterstützung brauchen oder Sie sich von Profis beraten lassen wollen: Wir von der RYSIT Consulting GmbH verstehen das Sicherheitsthema immer als essentiellen Bestandteil unserer EDV Betreuung. Zusammen können geeignete Schutzmechanismen gegen diese Bedrohung gesetzt werden, um das Risiko zu minimieren.

Sollten Sie noch Fragen haben stehen wir Ihnen gerne aktiv als Ansprechpartner zur Verfügung. Nutzen Sie dafür das Kommentarfeld auf https://www.rysit.at , schreiben Sie uns eine E-Mail an office@rysit.at oder rufen Sie uns direkt an (+43 1 361 95 00).

Nachwort:

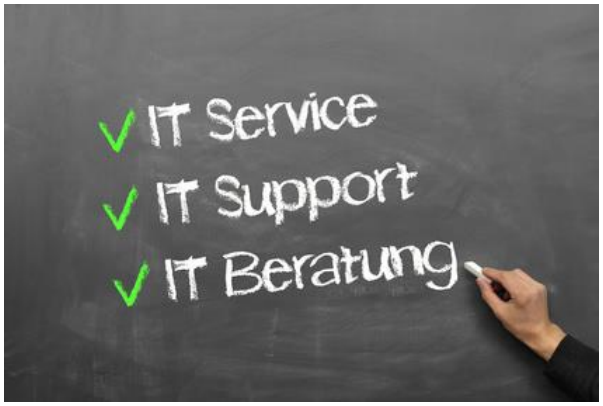
Nochmals vielen Dank für den Download dieses eBooks. Wir hoffen, dass Sie nun ein besseres Verständnis für die aktuellen IT-Sicherheits-Bedrohungen und damit verbunden Gegenmaßnahmen bekommen haben.

Sofern Sie unseren aktuellen RYSIT-Newsletter noch nicht kennen, möchten wir Sie an dieser Stelle darauf aufmerksam machen. Hier bekommen Sie regelmäßig Infos, Hilfe, Tipps & Tricks rund um die EDV und IT für Firmen von Ihrem IT-Profi.

Die Anmeldung erfolgt hier: https://www.rysit.at/news

Wenn Sie über dieses eBook hinaus wissen möchten, ob Ihr Netzwerk und Ihre Computer gegen die aktuellen Bedrohungen abgesichert sind, haben wir hier nun ein exklusives Angebot für Sie:

Sichern Sie sich jetzt unseren IT-Check für 149,- EUR statt 249,- EUR!



Nutzen Sie die Gelegenheit und buchen Sie einen IT-Check unter Angabe des **Bestellcodes „eBook“** und sparen Sie 100,- EUR.

Das Paket umfasst:

- ein persönliches Gespräch bei Ihnen vor Ort (ohne Anfahrtskosten in Wien, NÖ, Burgenland), bei dem wir die wichtigsten Bereiche rund um Ihre IT mit Ihnen gemeinsam analysieren und Sie über Möglichkeiten informieren, wie Sie Ihr System mit (teilweise sehr) geringem Aufwand optimieren können
- einen kompletten technischen Check Ihrer aktuellen IT-Infrastruktur
- die Erstellung einer mehrseitigen Dokumentation
- sowie ein maßgeschneidertes Konzept wie Sie ggf. Ihre EDV optimal verbessern können

Nutzen Sie dafür das Kontaktformular auf https://www.rysit.at/it-check/ , schreiben Sie uns eine E-Mail an office@rysit.at oder rufen Sie uns direkt an (+43 1 361 95 00).

Impressum:

RYSIT Consulting GmbH

Franz-Josefs-Kai 39/32

1010 Wien

Österreich

E-Mail: office@rysit.at

Website: https://rysit.at

Facebook: https://www.facebook.com/rysitat

Bildnachweise:

Nutzungshinweise für dieses eBook

Die in diesem eBook beschriebenen Maßnahmen und Vorgehensweise basieren auf persönlichen Erfahrungen, die wir im Rahmen unserer Tätigkeit im Bereich EDV Betreuung von kleinen und mittelständischen Unternehmen in den vergangenen Jahren gemacht haben. Aus diesem Grund können wir bestätigen, dass die erläuterten Maßnahmen und Vorgehensweisen im Rahmen der für sie beschriebenen Merkmale funktionieren. Für unsere Kunden haben sich die Nutzung der in diesem eBook beschriebenen Maßnahmen bewährt – wir weisen aber darauf hin, dass Resultate bei der individuellen Nutzung im Einzelfall variieren und deshalb weder vorhergesagt noch garantiert werden können.

Wir garantieren die Qualität aller in diesem eBook beschriebenen Tipps zum Zeitpunkt der erstmaligen Veröffentlichung, können aber keine Verantwortung für die Folgen (welcher Art auch immer) ihrer Anwendung übernehmen. Wir haben alle Anstrengungen unternommen, damit sichergestellt ist, dass die Informationen in diesem eBook korrekt sind. Als Nutzerin oder Nutzer liegt die Verantwortung für alle Konsequenzen, die sich aus der Inanspruchnahme des eBooks ergeben, ausschließlich bei Ihnen. Wir behalten uns das Recht vor, dieses eBook zu aktualisieren oder auch zu ändern, sofern es erforderlich ist. Kein Teil dieses Buchs darf ohne unsere ausdrückliche und schriftliche Genehmigung vervielfältigt oder in irgendeiner Weise reproduziert werden. Das eBook ist ohne Ausnahme für den Eigengebrauch bestimmt.