Security Guide

für Unternehmen

panda

Inhalt

Wir könnten Ihnen eine Menge Gründe für die Erstellung dieses Security Guides nennen. Doch wir denken, dass einer ausreichend ist: Mehr als 90 Prozent der kleinen und mittelständischen Unternehmen in Europa waren schon einmal Opfer eines IT-Angriffs.

In den meisten Fällen kam es dabei zum Diebstahl sensibler Informationen.

Denken Sie also nicht, dass Ihr Unternehmen für Cyberkriminelle nicht attraktiv genug ist.

Schützen Sie sich, bevor es zu spät ist...

Mehr als 90 Prozent der kleinen und mittelständischen Unternehmen in Europa waren bereits Ziel von IT-Attacken*

*Quelle: Shopper Software Seguridad en Pymes, Nielsen, April 2015

2

—

Wo liegen die größten Gefahren und wie können Sie Ihre Firma schützen?

Social Engineering

Eines der größten Sicherheitsrisiken für Unternehmen ist der Mensch: Der Begriff ‚Social Engineering' bezeichnet Angriffe, bei denen die Mitarbeiter einer Firma mit einem Trick dazu gebracht werden, normale Sicherheitsvorkehrungen zu umgehen und so sensible Informationen preiszugeben.

Dabei greifen Cyberkriminelle die Firmen meist auf zwei Arten an:

Beispielsweise kontaktiert der Angreifer einen Mitarbeiter per Telefon und schildert ein angeblich dringendes Problem, das nur durch den sofortigen Zugriff auf das Netzwerk behoben werden kann. Da die meisten Menschen in Notsituationen helfen wollen oder schlicht Angst haben, in einer für sie unbekannten Situation falsch zu reagieren, geben sie in solchen Fällen häufig sensible Informationen heraus.

Telefon

Wie können Sie sich schützen?

Internet

Die am weitesten verbreitete Social Engineering-Methode ist jedoch das sogenannte Phishing. Bei diesem Betrugsversuch enthalten die potenziellen Opfer E-Mails, die angeblich von bekannten Banken, Telefongesellschaften oder anderen Firmen stammen und die den Empfänger dazu auffordern, bestimmte (vertrauliche) Daten preiszugeben, weil beispielsweise eine Rechnung vermeintlich nicht bezahlt wurde oder Zugangsdaten bestätigt werden müssen.

Mitarbeiter schulen

Die beste Methode, um Angriffen vorzubeugen, ist, die Mitarbeiter zu schulen und sie über Social-Engineering-Taktiken aufzuklären.

Misstrauisch sein

Es ist empfehlenswert, ein gesundes Misstrauen zu hegen gegenüber allzu neugierigen Fragen. Cyberkriminelle geben normalerweise auf, wenn sie denken, dass ihnen das Opfer nicht vertraut.

Alles infrage stellen

Wir sollten die Person, die sensible oder interne Informationen von uns bekommen möchte, immer fragen, warum sie die Informationen benötigt. Die Mehrheit der Social-Engineering-Angriffe scheitert, wenn Fragen gestellt werden.

Quellen überprüfen

Wenn wir bezüglich einer Anfrage, die normalerweise nicht per E-Mail erfolgt, misstrauisch sind, dann sollten wir sie telefonisch überprüfen.

Wenn wir uns zum Beispiel in einem Kundengespräch oder auf Messen mit jemandem unterhalten, den wir nicht kennen, und der ungewöhnlich intime Fragen stellt, sollten wir denjenigen bitten, sich auszuweisen.

Nein sagen

Wenn ein Cyberkrimineller Social Engineering anwendet, weicht er gewöhnlich von den Normen des Geschäftslebens ab oder bringt das Opfer dazu, dies zu tun. Sich an die Firmenrichtlinien zu halten, ist der beste Schutz.

E-Mail

Wie können Sie sich schützen?

Viele der Cyberattacken auf Unternehmen erfolgen über E-Mails, die bereits vermeintliche Insider-Informationen über die Firma enthalten. Bei diesem sogenannten ‚Spear-Phishing' suchen die Hacker vorab in öffentlichen Datenbanken wie Facebook oder auf Unternehmenswebseiten nach möglichst detaillierten Firmeninformationen, die sie in ihren E-Mails verwenden können. Ziel ist es, bei den Empfängern den Eindruck eines legitimen Schreibens zu erwecken und auf diese Weise zum Klick auf einen Phishing-Link innerhalb der E-Mail zu verleiten.

Wie beim Social Engineering sollten die Mitarbeiter im Bereich IT-Sicherheit geschult werden, um riskantes Verhalten im Umgang mit Firmenmails zu vermeiden.

Verschlüsseln Sie Firmen-E-Mails. Damit Unternehmen sensible Informationen kontrollieren und diese auch nicht über private E-Mail-Konten abgegriffen werden können, sollten berufliche E-Mails stets verschlüsselt werden.

Alte E-Mails löschen. Wenn Sie Tausende von E-Mails haben, die Sie für wichtig halten, sollten Sie diese auf einer externen Festplatte, in einer Datenbank oder in der Cloud speichern. Sie können diese dann von Ihrem E-Mail-Konto entfernen.

Wenn Sie ein Passwort festlegen müssen, stellen Sie sicher, dass es komplex ist und niemand es erraten kann.

Seien Sie vorsichtig, wenn Sie sich an öffentlichen Computern einloggen. Achten Sie darauf, sich auszuloggen, bevor Sie den Computer verlassen. Sie könnten sonst leicht zu verfolgende Spuren für Cyberkriminelle hinterlassen. Am besten ist es, das Firmen-Mail-Konto nur zu nutzen, wenn man an einem sicheren Computer arbeitet.

Geben Sie nicht jedem Ihre Adresse. Sie sollten sie auch nicht auf öffentlichen Webseiten hinterlassen. Betrüger warten stets auf eine passende Gelegenheit.

Seien Sie vorsichtig bei E-Mails, die Sie auffordern, ein neues Passwort für höhere Sicherheit zu vergeben. Wenn Sie Ihr Passwort ändern müssen, gehen Sie auf die Webseite des E-Mail-Providers und tun Sie es dort. Nutzen Sie auf keinen Fall den Link aus einer E-Mail.

Öffnen Sie keine E-Mails, die von unbekannten oder verdächtigen Quellen stammen.

Nutzen Sie das Firmen-Mail-Konto nur als Arbeitsmittel. Für persönliche Zwecke sollte es tabu sein.

Telearbeit / Homeoffice

Die Möglichkeit, von zu Hause aus zu arbeiten, bietet Arbeitnehmern mehr Flexibilität und erhöht ihre Produktivität.

Aber wie sieht es mit der Sicherheit aus?

Wenn Mitarbeiter im Homeoffice arbeiten, haben sie nicht dieselbe Sicherheit wie im Unternehmen, da die Software zu Hause gewöhnlich nicht so gut geschützt ist wie im Firmennetzwerk.

So kann es auf unterschiedliche Art und Weise zu Datenverlust kommen: Ein Fehler auf dem Computer tritt auf, der Dateien löscht, von denen es keine Sicherheitskopien gibt. Ein Passwort wird gestohlen. Der Computer wird von Cyberkriminellen gehackt.

Wie können Sie sich schützen?

Es ist unerlässlich, dass es eine Unternehmensrichtlinie gibt, die festlegt, wie man in Bezug auf die Sicherheit von zu Hause aus arbeitet.

Die Nutzung von Remote-Desktops ist eine Lösung. Mit ihnen ist es möglich, Datenverlust zu vermeiden. Die Mitarbeiter können sich direkt mit dem Firmenserver verbinden, auf dem alle Informationen und Sicherheitskopien automatisch gespeichert werden.

Ein weiterer wichtiger Punkt ist die Passwortsicherheit. Der Diebstahl des Zugangscodes eines Mitarbeiters könnte katastrophal sein, da dies viele Daten gefährdet. Hier gilt es vor allem, zwei Punkte zu berücksichtigen: Nutzen Sie starke Passwörter und ändern Sie diese häufig. Verwenden Sie einen Passwort-Manager, um die Zugangscodes zu schützen.

Verschlüsseln Sie vertrauliche Informationen. Sollte ein Laptop abhandenkommen oder gestohlen werden, bedeutet dies nicht automatisch, dass die Informationen für andere zugänglich sind. Indem Dateien oder sogar die gesamte Festplatte über das Betriebssystem verschlüsselt werden, kann man dieses Risiko umgehen.

Die Telearbeit nimmt dank neuer Technologien schnell zu. Das bedeutet jedoch nicht, dass die digitale Sicherheit gefährdet sein muss. Die richtige Anti-Malware-Technologie bietet entsprechende Tools, um Daten zu schützen, wenn Mitarbeiter im Homeoffice arbeiten.

Cloud

Ihre Benutzerfreundlichkeit hat dafür gesorgt, dass wir immer stärker miteinander vernetzt sind.

Wenn Sie jedoch virtuelle Speicher nutzen, um Ihre Geschäftsdaten aufzubewahren und zu teilen, könnte es sein, dass die Sicherheitsmaßnahmen nicht ausreichen.

Wie können Sie sich schützen?

Erstellen Sie sichere Passwörter. Sichere Passwörter gehören zu den Grundvoraussetzungen für die IT-Sicherheit. Kombinieren Sie Groß- und Kleinbuchstaben, Zahlen, Symbole und nutzen Sie verschiedene Passwörter für unterschiedliche Konten.

Achten Sie auf die Datenverschlüsselung. Einige virtuelle Speicherdienste bewahren unsere Dokumente verschlüsselt auf.

Dropbox tut dies nicht, der Online-Speicherdienst Mega schon. Jedoch ist auch dieser nicht perfekt: Mega speichert eine Kopie des Codes, um die Daten auf seinen Servern zu entschlüsseln, was nicht 100-prozentig sicher ist. Sie sollten die Daten daher besser selbst verschlüsseln, bevor Sie sie in der Cloud speichern.

Bei Dropbox und Google Drive können Sie die Zwei-Faktor-Authentifizierung aktivieren. Dieses System kombiniert das von Ihnen genutzte Passwort mit einem weiteren, das auf Ihr Mobilgerät gesendet wird (per SMS oder App), und sorgt so für eine zweite Sicherheitsschicht.

Mobilgeräte

Eine Firma ist nicht sicher, wenn sie nur die internen IT-Geräte schützt. Heutzutage ist es unerlässlich, eine Sicherheitsstrategie für firmeneigene Mobilgeräte zu haben. Diese sollte den Schutz der Geräte sowie der Informationen und Applikationen, die auf ihnen genutzt werden, gewährleisten.

Laut einer Studie über den Schutzstatus von kleinen und mittelständischen Unternehmen, die das Marktforschungsinstitut Nielsen 2015 im Auftrag von Panda Security durchgeführt hat, haben 25 Prozent der firmeneigenen Tablets keine Sicherheitssoftware. Bei Smartphones sind es sogar 35 Prozent. Diese Zahlen zeigen, warum viele der aktuellen Angriffe gegen Mobilgeräte gerichtet sind.

Zusätzlich zum Schutz besteht eine weitere Anforderung an die mobile Sicherheitsstrategie: Sie soll die Beweglichkeit und die Dynamik des Unternehmens nicht behindern, welche die Nutzung von Mobilgeräten bietet.

Wie können Sie sich schützen?

Zunächst muss sichergestellt werden, dass auf den Mobilgeräten eines Unternehmens eine moderne Sicherheitssoftware installiert ist. Da dies oftmals noch nicht der Fall ist, rückten mobile Devices in jüngster Zeit vermehrt in den Fokus von Cyberkriminellen.

Die Nutzeridentifikation bedarf besonderer Aufmerksamkeit, denn die Wahrscheinlichkeit, dass ein Handy oder Tablet in fremde Hände gerät, ist wesentlich größer als bei firmeninternen IT-Geräten. Bei vielen Mobilgeräten können wir unseren Fingerabdruck zur Identifikation nutzen. Firmen sollten ihre Mitarbeiter darin schulen, derartige Tools zu verwenden und ihnen außerdem vermitteln, wie sie sich im Falle von verlorenen oder gestohlenen Geräten zu verhalten haben.

Seien Sie vorsichtig bei Software von Drittanbietern: Viele Berufstätige installieren auf dem beruflich genutzten Mobilgeräten Apps aus fragwürdigen Quellen. Auch wenn diese auf den ersten Blick vertrauenswürdig erscheinen, könnten sie von Cyberkriminellen gefälscht sein. Das gefährdet die Sicherheit des Unternehmens.

Mobilgeräte müssen so eingerichtet werden, dass sie unsichere WLANs meiden. Den Anwendern sollten Sie empfehlen, die Bluetooth-Option grundsätzlich zu deaktivieren, damit sie keine (bösen) Überraschungen erleben.

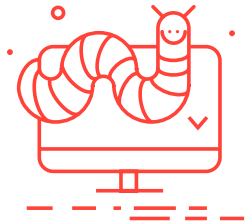
3

—

Die gefährlichsten Arten von Malware

Unter einem Scam versteht man einen großangelegten Online-Betrug, dessen Ziel es ist, die Opfer zu einer Geldzahlung zu bewegen, zum Beispiel um eine angebliche Gewinnspielprämie oder eine erfundene Erbschaft zu erhalten.

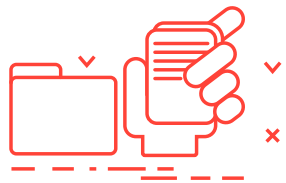
Ein Computerwurm ist ein Schadprogramm, das sich selbst vervielfältigen kann und so all Ihre Computer im Netzwerk infiziert. Würmer verbrauchen einen Großteil der Netzwerkressourcen und können so zu einer Überlastung führen.



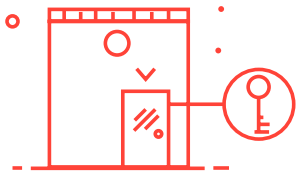
Über gefälschte E-Mails, Webseiten oder SMS werden Daten von Internetnutzern abgefangen. Ziel dieser Art von Betrug ist es, an persönliche Zugangsdaten und Passwörter für Bankkonten und ähnliches zu gelangen und diese zu missbrauchen.

Die gefährlichsten Arten von Malware (I)

- Scam
- Wurm
- Phishing
- APT
- Backdoor
- Keylogger

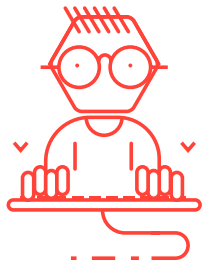


Ein APT bzw. Advanced Persistent Threat (deutsch: fortschrittliche andauernde Bedrohung) ist ein zielgerichteter Angriff auf Ihre IT-Infrastruktur. Hierbei verschafft sich eine unautorisierte Person Zugriff auf Ihr Netzwerk und hält sich dort möglichst lange unentdeckt auf, um so viele sensible Daten wie möglich zu stehlen.

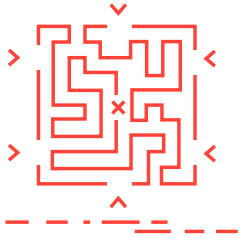


Durch das Öffnen einer „Hintertür“ werden Sicherheitsmaßnahmen umgangen, um die Kontrolle über Ihr Computersystem zu übernehmen.

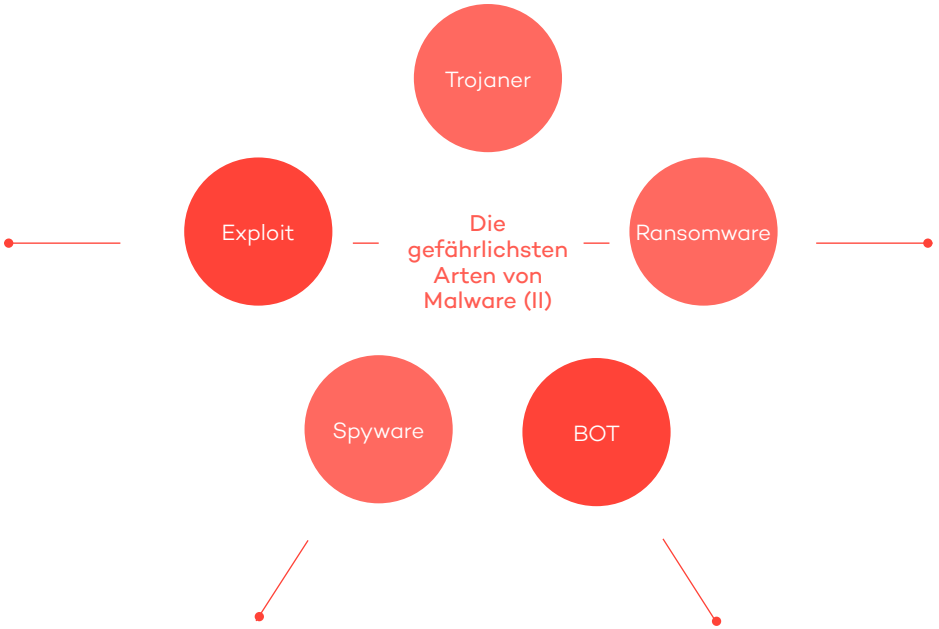
Sie protokollieren alle Eingaben des Benutzers an der Tastatur. Keylogger werden von Cyberkriminellen genutzt, um an vertrauliche Daten wie Kennwörter oder PINs zu gelangen.



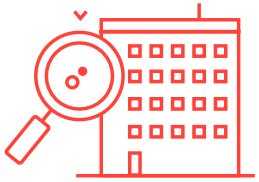
Sie installieren verschiedene Anwendungen, sodass Hacker die Kontrolle über den Computer übernehmen können. Trojaner kontrollieren Ihre Dateien und stehlen vertrauliche Informationen.



Es nutzt Sicherheitslücken oder Schwachstellen in den Kommunikationsprotokollen aus, um in Ihren Computer zu gelangen.

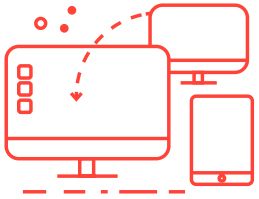


Sie blockiert den PC, entzieht dem Anwender die Kontrolle über seine Daten und Arbeitsprozesse, verschlüsselt Dateien und fordert ein Lösegeld für die Rückgabe der Daten.



Sie sammelt Namen, Zugangsdaten, Passwörter und alle Arten von Informationen über Ihre Firma.

Das ist ein Computerprogramm, das bestimmte Aufgaben automatisiert und selbstständig ausführt. Bots werden zum Beispiel für das Sammeln von E-Mail-Adressen eingesetzt.

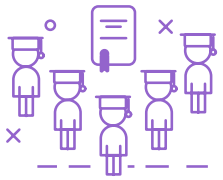


4

Verhaltensregeln für mehr Cyber-Sicherheit in Ihrem Unternehmen

Verhaltensregeln für mehr Cyber-Sicherheit

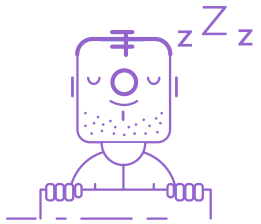
1 Schulen Sie Ihre Mitarbeiter Ihr Wissen über Sicherheit wird Ihre Firma schützen.



2 Achten Sie auf den Schutz von Mobiltelefonen und Tablets, nicht nur auf die Sicherheit von PCs.

3 Seien Sie besonders vorsichtig bei Links, die in E-Mails enthalten sind.

4 Nutzen Sie eine Sicherheitslösung, die in der Lage ist, fortschrittliche Bedrohungen zu erkennen und zu blockieren.



5 Verschlüsseln Sie Ihre wertvollsten Daten.

6 Nutzen Sie Remote-Desktops für Telearbeit.

7 Installieren Sie keine fragwürdigen Apps von Drittanbietern in Ihrem Firmennetzwerk.

8 Fertigen Sie regelmäßig Sicherheitskopien von wichtigen Daten an.

9 Vorsicht bei öffentlichen Wi-Fi-Netzwerken, wenn Sie ein Firmengerät nutzen.

10 Erstellen Sie komplexe Passwörter, und ändern Sie diese möglichst häufig.

Lassen Sie sich von uns schützen!

Endpoint Protection Plus

Halten Sie Ihr komplettes Firmennetzwerk frei von Viren und Spam. Endpoint Protection Plus ist eine intuitive und ressourcenschonende Endpoint-Sicherheitslösung inklusive Web- und Spam-Filter. Der zentralisierte und unterbrechungsfreie Schutz bietet flächendeckende Sicherheit auf allen Devices. Endpoint Protection Plus schützt Windows-, Mac- und Linux-Workstations, einschließlich führender Virtualisierungssysteme, Laptops und Smartphones.

Ganz einfach, oder?

Mehr erfahren

Adaptive Defense 360

Maximaler IT-Schutz für Unternehmensnetzwerke. Adaptive Defense 360 kombiniert erstmals zwei hochentwickelte Cyber-Security-Technologien in einer einzigen Konsole: Endpoint Detection and Response (EDR) und Endpoint Protection (EPP). Auf diese Weise überwacht, protokolliert und klassifiziert Adaptive Defense 360 alle laufenden Anwendungen auf den Firmen-Endpoints und erkennt und blockiert auch die Malware, die von anderen Systemen nicht erkannt wird.

Uneingeschränkte Transparenz, absolute Kontrolle!

Mehr erfahren


panda