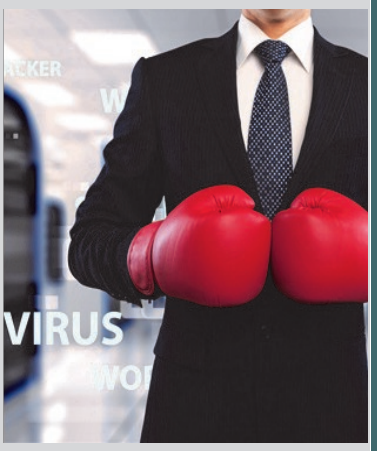
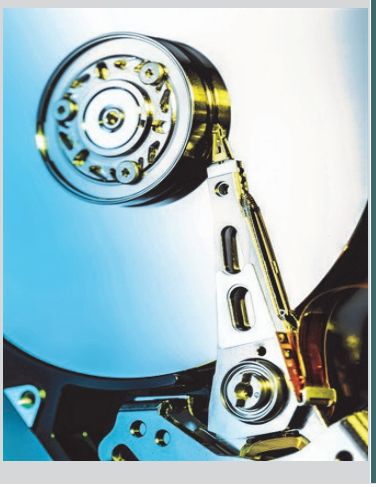
RoCas Heilpraxis

RoCas GbR.
Guido Rochow & Astrid Casteel
Hotline: +49 (2163) 8998088
Fax: +49 (2163) 8998087
Web: www.rocas-heilpraxis.de
Mail: heilpraxis@rocas.de



Die wichtigsten Maßnahmen:

- Backups anlegen
- Aktueller Virenscanner
- Updates installieren
- Mailanhänge prüfen
- Gesundes Misstrauen
- Sichere Passwörter



Viren, Trojaner & Co.

Wie schütze ich meine Daten vor Cyberattacken?

Guido Rochow
Chefentwickler der
RoCas Heilpraxis

Sicherlich werden Sie schon einiges in den Nachrichten über immer stärker aufkommende Cyberattacken und Verschlüsselungstrojaner gehört haben. Die Verunsicherung ist groß, was denn zu tun ist und so werden wir auch im Support häufig gefragt, ob es wirklich so gefährlich ist. Da können wir nur „ja" sagen, aber mit ein paar Maßnahmen und etwas Vorsicht kann man das Risiko deutlich minimieren und im schlimmsten Fall auf ein Backup zurückgreifen. Ganz ohne Schutz und Backups, kann so etwas allerdings zum Alptraum werden, wenn die Geschäftsdaten verschlüsselt sind, oder (wie in seltenen Fällen schon geschehen) damit gedroht wird, die abgegriffenen Daten zu veröffentlichen. Hier sollen die wichtigsten Maßnahmen möglichst einfach und kurz erklärt werden.

Backups anzulegen ist eine der wichtigsten Vorgehensweisen gegen alle Arten von Datenverlusten wie Verschlüsselung oder Festplattenproblemen. Dies kann man mit Bordmitteln anlegen, aber komfortabler mit einer Backupsoftware, und die muss nicht mal teuer sein. Wichtig dabei, das Laufwerk immer nach dem Backup zu trennen, das heißt, die USB Verbindung in Windows aufheben und das Laufwerk auch physikalisch vom Rechner trennen, bei Netzlaufwerken ebenso die Kabelverbindung lösen, denn es gibt einige Trojaner, die die Daten auch über diese Verbindungen hinweg verschlüsseln. Besonders sicher ist es, abwechselnd zwei verschiedene Backuplaufwerke zu nutzen, da – auch während ein Backup geschrieben wird – ein Trojaner zuschlagen könnte (der kann schon vorher auf der Festplatte sein und nur darauf warten, dass ein weiteres Laufwerk angeschlossen wird) und so hätte man immer noch das vorherige. Falls Sie kein zweites Backuplaufwerk anschaffen möchten, ist es sehr ratsam, zumindest die Datenbanken der Abrechnungs- und Verwaltungsprogramme zusätzlich auf USB-Sticks zu sichern. Wie oft sollte man einen Rechner sichern? Gegenfrage, auf wie viele Daten können Sie verzichten? Praktikabel ist die Vollsicherung (kompletter Rechner) wöchentlich und die Datenbanken der Abrechnungs- und Verwaltungsprogramme täglich zu sichern.

Virenscanner sind unverzichtbar auf jedem Windows-Rechner und sollten natürlich immer aktuell sein. Hier gibt es von verschiedenen Herstellern verschiedene Angebote, die Weiteres absichern, wie Onlinebanking, Browsersicherheit, Spamfilter, Firewall, etc. und das macht durchaus Sinn. Allerdings kann kein Produkt einen sehr neuen Virus oder Trojaner finden, daher sollte der Scanner nicht die einzige Lösung sein, später dazu mehr. Die Bordmittel schneiden in Tests nicht sehr überzeugend ab.

Updates – hierüber haben Softwarehersteller die Möglichkeit, ihre Software weiter abzusichern, sowohl zum Betriebssystem als auch zu allen installierten Programmen (besonders Officeprodukte und Browser) sollten immer direkt, wo es möglich ist, automatisch aufgespielt werden. Microsoft gibt immer am zweiten Dienstag eines Monats neue Updates zum Betriebssystem, den eigenen Officeprodukten und Internet Explorer bzw. Edge heraus (Patchday) die wirklich zügig installiert werden sollten. Schauen Sie bitte hin und wieder mal im Updateverlauf nach, ob auch wirklich die Updates installiert wurden (Sollte ein Update fehlgeschlagen sein, versuchen Sie bitte, es nochmals zu installieren und googeln Sie die KB-Nummer oder die Bezeichnung des Updates, um zu wissen, welchen Zweck das Update hat. Bitte nutzen Sie keine alten Produkte wie Vista, XP oder alte Officeprodukte, da Sie keine Updates mehr erhalten. Falls Sie einen anderen Browser als Internet Explorer oder Edge nutzen möchten, das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt immer wieder heraus, dass Chrome einer der sichersten Browser ist. Für Sie von Vorteil: Chrome updatet auch alle abhängigen Komponenten. Besonders zu erwähnen ist hier der sehr gefährliche Flash-Player, ein häufiges Angriffsziel, er sollte immer aktuell sein. Aber schauen Sie sich auch alle anderen installierten Programme an, kann man dort einstellen, dass Sie sich automatisch aktualisieren? Oder könnten Sie das Programm gegen ein anderes austauschen? Z.B. einen PDF-Viewer, auch hier ist Aktualität sehr wichtig und es gibt einige kostenlose, die automatisch updaten können. Googeln Sie einfach Ihr installiertes Programm und Update, hier ist eigentlich immer eine hilfreiche Antwort zu finden.

RoCas Heilpraxis

RoCas GbR.
Guido Rochow & Astrid Casteel
Hotline: +49 (2163) 8998088
Fax: +49 (2163) 8998087
Web: www.rocas-heilpraxis.de
Mail: heilpraxis@rocas.de

Bildquellen: Billionphotos, RoCas GbR.

Mailanhänge, einer der häufigsten Angriffsvektoren und daher sehr gefährlich. Seien Sie bitte besonders vorsichtig. Alle ausführbaren Dateien und dazu kann man auch Officedateien, wie Word und Excel zählen, sind potenziell virulent. Viele kennen die Dateiendungen der ausführbaren Dateien nicht und Windows zeigt sie auch je nach Einstellung nicht an. Bevor wir hier eine Liste veröffentlichen, die Sie am besten auch noch auswendig lernen, ein einfacherer Weg. Eine kostenlose Seite im Internet, **www.virustotal.com**, bietet die Möglichkeit, solche Dateien hochzuladen und von über 50 Scannern durchsuchen zu lassen. Wenn schon ein Teil der Scanner etwas an dieser Datei finden, bitte nicht öffnen, sondern direkt löschen. Die Scanner auf der Seite sind sehr aktuell, aber immer gilt noch, wie auch beim installierten Virenscanner auf Ihrem Rechner, dass die Virensignatur bekannt sein muss, um den Schädling zuverlässig zu finden und diese Signaturen können die Cyberkriminellen auch schnell ändern. Es bleibt also eine Art Wettrüsten. Die Seite ist ein Zusammenschluss der Schutzsoftwarehersteller, um auch an neue Virensignaturen zu gelangen, sie helfen also nicht nur sich selbst, sondern auch, neue Viren zu entdecken. Ein weiterer Vorteil: Sie können auch eine URL, also die Adresse einer Internetseite eingeben und so vor dem Besuch feststellen, ob Sie auf der Seite Schadsoftware erwartet. Eine Infektion geht auch, ohne dass Sie irgendetwas anklicken (drive by), also lieber vorher mal prüfen lassen. Ein Trugschluss, den wir immer wieder hören: PDF Dateien und Anhänge von bekannten Absendern seien sicher.

Dies hat sich leider bei vielen zur festen Meinung entwickelt, ist aber so nicht richtig. Sollte Ihr PDF-Programm aktuell sein und Sie der Datei keine weiteren Rechte erteilen, dann ist eine PDF sicherer als z.B. eine Word-Datei, die Makros enthalten kann (Die Ausführung von Makros unbedingt in den Officeprodukten ausschalten und auch auf Nachfrage nicht gewähren). Ist der Rechner des bekannten Absenders von einem Virus befallen, dann sendet der womöglich Viren an alle gespeicherten Kontakte, dies ist schon mehrfach vorgekommen, ebenso können Mailadressen gefälscht oder extrem ähnlich sein, z.B. versteckt sich irgendwo ein Punkt in der Adresse, den Sie eventuell nicht direkt sehen, also auch bei bekannten Absendern Vorsicht walten lassen.

Mahnungen kommen per Post.

Ein häufiger Infektionsweg ist eine Mahnung als Word- oder ZIP-Datei, da eine Mahnung per Mail nicht rechtswirksam ist, werden diese normalerweise nicht per Mail geschickt. Lassen Sie sich nicht blenden, wenn im Mailtext Ihre persönlichen Daten stehen und das Ganze angeblich von einem Rechtsanwalt oder Inkassobüro stammt. Wenn Sie etwas wirklich nicht bezahlt haben und es ernst wird, kommen solche Dinge immer noch per Post, oftmals per Einschreiben. Reagieren Sie also nur mit Löschen auf eine solche Mail. Es ist zu beobachten, dass die sogenannten Spammails immer raffinierter erstellt werden, damit sie unbedingt mit samt Anhängen geöffnet werden. Je reißerischer der Inhalt und je stärker die Drohung (Inkasso), desto mehr können Sie davon ausgehen, dass es sich um eine Spammail handelt. Aber auch Links in Mails können auf verseuchte Seiten leiten, dies ist ebenso gefährlich. Gehen Sie lieber manuell auf die Seite, indem Sie die Adresse selber in den Browser eingeben und klicken Sie nichts (Bilder, Buttons, Links) innerhalb eines Mailtextes an. Oftmals sollen solche Links zum Login in ein Kundenportal führen, dies kann gefälscht sein um an Ihre Zugangsdaten zu gelangen. Also wenn Sie sich z.B. bei Ihrer Bank einloggen möchten, dann immer das Onlineportal selber aufrufen. Oftmals werden Logos und Mailadressen von bekannten großen Unternehmen, von denen Sie eine Rechnung oder Mail erwarten (Telekom, 1&1, DHL, DPD, etc.) sehr gut nachgeahmt und die Zeiten in denen diese Spammails immer durch schlechtes Deutsch zu erkennen waren, sind leider vorbei.

Misstrauen schützt.

Bleiben Sie misstrauisch bei allem, was Sie anklicken und vor allem, wenn Sie per Dialog nach weiteren Rechten gefragt werden. Schätzen Sie am besten alle Dinge, die aus dem Internet stammen, und damit sind auch Mailanhänge gemeint, als virulent ein, bis Sie sich vom Gegenteil überzeugt haben. Weitere Informationen finden Sie beim Bundesamt für Sicherheit in der Informationstechnik (BSI), hier besonders: BSI für Bürger und Siba (Deutschland sicher im Netz e.V.).

Ein weiteres Manko stellen unsichere Passwörter dar.

Bitte nutzen Sie mindestens achtstellige, die aus Zahlen, Buchstaben und Sonderzeichen bestehen und nicht auf Geburtsdaten o.ä. hinweisen. Ebenso sollte für jeden Dienst, bzw. Anmeldung ein eigenes genutzt werden. Hierfür kann man Passwortmanager benutzen, oder sein Passwort etwas variieren und mit Merksätzen arbeiten. Z.B.: Meine erste Katze hieß Kira, sie wurde neunzehn Jahre alt. Daraus könnte man als Passwort M1KhKira,sw19Ja ableiten. Nehmen Sie hierfür Informationen, die nicht in sozialen Netzwerken gepostet wurden, oder die jeder kennt. Erweitern Sie das Passwort noch um den Dienst, bei dem Sie sich anmelden möchten, für z.B. ebay könnte man noch yaB anfügen, usw. Speichern Sie Passwörter nicht auf dem Rechner, es sei denn, Sie haben ein spezielles Programm dafür. Wir unterstützen und beraten unsere Kunden gerne auch zu diesen Themen und haben alle nötigen Produkte von verschiedenen Herstellern im Angebot. Außerdem veröffentlichen wir besondere Vorfälle oder sehr wichtige Informationen aus diesem Bereich auf unserer Internetseite: **www.rocas-heilpraxis.de** unter „Aktuelles“.