SOPHOS

5 Ausreden, um nichts für die Sicherheit am Computer tun zu müssen – und wie man sie entkräftet!

Seien wir mal ehrlich: viele Computer und Webseiten sind schneller und einfacher zu nutzen, wenn nichts für die Sicherheit getan wird. Das spart schon mal mehrere Minuten am Tag! Anhänger dieser Vorgehensweise sind natürlich auch um Ausreden nicht verlegen und ich kann aus eigener Erfahrung ein Lied davon singen, wie schwer es ist, jemanden vom Gegenteil zu überzeugen. Deshalb hier die Top-5-Ausreden, die ich häufig und nicht nur von Privatpersonen, sondern auch von kleinen Unternehmen zu hören bekomme. Aber IT-Sicherheit ist kein Nice-to-have sondern ein Must-have.

Ausrede Nr. 1: Ich bin zu unwichtig, als dass sich jemand für meine Daten interessiert!

Die landläufige Meinung ist, dass Cyberkriminelle einfach nicht an der örtlichen Autowerkstatt oder der aufstrebenden Produktionsstätte für achteckige Bierdeckel interessiert sind. Warum sollten die Gauner sich auch mit einem Kleinstunternehmen oder gar einer Privatperson zufrieden geben, wenn sie genauso gut Konzerne mit zigfachem Millionenumsatz ins Visier nehmen können? Klingt logisch, aber in unserem Fall greift eher das Sprichwort „Kleinvieh macht auch Mist“. Viele Großkonzerne machen ihre Umsätze nicht mit 10 Deals zu je 1 Milliarde Euro, sondern vielmehr mit 1 Milliarde Deals zu je 10 Euro. Und genau dieses Verhältnis von kleinem Wert und großer Anzahl ist für die Cyberkriminellen am attraktivsten. Sie schöpfen also lieber unzählige Privatpersonen oder Kleinstunternehmen ab, anstatt ein vermeintlich besser geschütztes Großunternehmen anzugreifen. Beispiele gefällig? Die CryptoLocker-Gang erleichterte alleine in Großbritannien über 100.000 Nutzer um jeweils rund 250 Euro und die Spamming-Industrie würde liebend gerne Ihren Computer übernehmen, um ihn dazu zu nutzen, millionenfach Spam in die Welt zu schicken.

Aus Perspektive der Cyberkriminellen sind wir alle potenzielle Opfer. Wir sind es uns, aber auch allen anderen Internetnutzern schuldig, uns bestmöglich zu schützen und den Verursachern von Malwareattacken das Leben so schwer wie möglich zu machen.

Ausrede Nr. 2: Mit der aktuellsten Software funktioniert mein Drucker nicht mehr!

Ok, ok, es muss nicht immer der Drucker sein. Tatsächlich ist es nicht einmal immer die Hardware, die Probleme bereitet. Immer häufiger muss veraltete Software als Ausrede herhalten, um im Morast der Unsicherheit zu verweilen. In letzter Zeit steht vor allem Windows XP hoch im Kurs, von dem sich viele einfach nicht trennen wollen und damit auch keine offiziellen Sicherheits-Updates mehr erhalten. Dieses Verhalten ist dann akzeptabel, wenn ältere und nur kostenintensiv zu ersetzende Geräte wie beispielsweise eine CNC-Fräse, die lediglich auf XP verlässlich läuft, im Einsatz sind. Wer allerdings nur einen stinknormalen PC oder Laptop sein eigen nennt, muss sich fragen, ob der Mehrwert eines angestaubten Druckers das Risiko nicht gepatchter Software rechtfertigt. Es muss jedem klar sein, dass Sicherheitslücken, die schon seit längerer Zeit bekannt sind, von den Hackern zuerst ausgenutzt werden, da Sie hier die effektivsten Angriffsmethoden haben.

Jedes Mal, wenn Sie weiter hinter den aktuellen Sicherheits-Updates einer Software zurückfallen, werden Sie zu einem noch attraktiveren Ziel für Cyberkriminelle.

Ausrede Nr. 3: Ich habe einen Mac!

Gute Wahl, habe ich auch! Aber egal welchen Computer Sie besitzen, oder welche Software installiert ist – wenn das Gerät verloren geht oder gestohlen wird, sind die darauf befindlichen Daten in fremden Händen. Denn selbst wenn die meisten gestohlenen Laptops schnell neu aufgesetzt und weiter verkauft werden, gibt es immer noch eine ganze Reihe von Geräten, die in die Hände von Datendieben geraten. Daten haben immer einen gewissen Wert, und Leute, die sich mit dem Extrahieren der richtigen Informationen auskennen, können eine Menge Geld damit machen. Kurze Rede, langer Sinn: die Marke des Computers gibt keinen Anlass zur Sorglosigkeit bei der Sicherheit der Daten.

Installieren Sie unbedingt eine Festplattenverschlüsselung auf Ihrem Laptop, wenn Sie ihn außer Haus nutzen. Dann bekommen die Datendiebe im Fall der Fälle nur geschredderten Müll.

Ausrede Nr. 4: Sicherheitssoftware macht meinen PC zur Schnecke!

Gerade in Bezug auf Festplattenverschlüsselung herrscht oftmals noch die irrige Meinung, dass sie PCs extrem verlangsamt. Diese Zeiten sind lange vorbei. Bei modernen Verschlüsselungslösungen wie BitLocker für Windows oder File Vault für OS X sind statistisch signifikante Performanceeinbrüche dank CPU-Verbesserungen so gut wie nicht mehr festzustellen. Auch Antivirus-Programme stehen im Ruf, die Rechnerleistung zu verschlechtern. Das hängt unserer Erfahrung nach aber primär damit zusammen, das viele Nutzer unnötiger Weise alle „Schalter“ des Programms aktivieren. Damit laufen oftmals redundante Kombinationen von Scanning-Optionen auf dem Rechner, der dann logischerweise mehr Arbeit als notwendig aufwenden muss. Auch sichere Passwörter und die Zweifaktor-Authentifizierung haben ihren Ruf als Zeitfresser weg. Aber mal ehrlich, die paar Sekunden sollten für ein großes Plus an Sicherheit doch wirklich drin sein.

Verzichten Sie nicht auf notwendige Sicherheitsanwendungen, nur um heute im Idealfall ein paar Minuten zu gewinnen. Dieser Fehler kann Ihnen schon Morgen ein Vielfaches an Zeit kosten.

Ausrede Nr. 5: Ich surfe nur zu sicheren Internetseiten!

Tatsächlich? Da stellt sich die Frage, woher Sie das wissen wollen. Wie können Sie im Voraus feststellen, ob eine Webseite sicher ist oder nicht? Internetnutzer sollten sich darüber im Klaren sein, das sogar legitime und bekannte Seiten mit Malware verseuchte Anzeigen beinhalten. Diese können ganz einfach über einen gehackten Provider eingespielt werden ohne dass der eigentliche Seitenbesitzer irgendetwas mitbekommt. Hier kann die Web-Filtering-Technologie weiterhelfen, da sie nicht nur die URLs der Internetseite checkt, sondern auch den kompletten Inhalt.

Gehen Sie nicht davon aus, dass jede Online-Gaunerei mit einem oder zwei Blicken erkennbar ist. Und selbst wenn Sie gestern noch eine sichere Seite ohne Probleme besucht haben, kann das heute schon ganz anders sein.

Die Moral von der Geschicht‘?
Ich habe hier exemplarisch fünf Ausreden für fehlende Sicherheit auf dem Computer aufgezählt. Natürlich ist die Liste noch viel länger, wenn es darum geht, die eigene Lethargie in punkto IT-Security schön zu reden. Aber bitte tun Sie das in Zukunft nicht mehr. Es gibt

sicherlich immer wieder Situationen, in denen bestimmte Vorkehrungen für Sie nicht praktikabel sind. In diesen Fällen haben Sie aber zumindest noch die Möglichkeit, potentielle Sicherheitslücken durch andere Vorkehrungen zu minimieren. Wenn Sie z.B. unbedingt XP behalten müssen, um Ihre Multimillionen-Euro-Maschine am Laufen zu halten, sollten Sie auf jeden Fall eine Firewall nutzen, um das gute Stück in eine sichere Ecke des Netzwerks zu verfrachten. Nichts zu tun ist wie immer die leichteste Übung, aber es ist auch die schlechteste. Nicht nur für Sie, sondern in Zeiten des World Wide Web auch für alle anderen.

Autor: Sascha Pfeiffer, Principal Security Consultant bei Sophos

Über Sophos
Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Sophos' Complete-Security-Lösungen als den besten Schutz vor komplexen IT-Bedrohungen und Datenverlust. Sophos bietet dafür preisgekrönte Verschlüsselungs-, Endpoint-Security-, Web-, Email-, Mobile- und Network Security-Lösungen an, die einfach zu verwalten, zu installieren und einzusetzen sind. Das Angebot wird von einem weltweiten Netzwerk eigener Analysezentren, den SophosLabs, unterstützt. Sophos hat seinen Hauptsitz in Boston, USA, und Oxford, Großbritannien. In Deutschland hat das Unternehmen seinen Hauptsitz in Wiesbaden und ist in Österreich und der Schweiz je an einem Standort vertreten. Weitere Informationen unter www.sophos.de.

Pressekontakt:
Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Christiane Capps, +49-174-3335550
Ulrike Masztalerz, +49-40-484434
sophos@tc-communications.de