SICHERHEIT

Zehn Punkte zum Schutz vor Malware

Die Virenflut hat ein enormes Mass erreicht, unabhängige Stellen berichten von über 350 000 neuen Viren pro Tag. Es reicht heute nicht mehr aus, das Antivirenprogramm einmal in der Woche zu aktualisieren.

AUTOR **ANDREAS WISLER**

Auch einmal pro Tag reicht nicht mehr aus – viele Programme aktualisieren sich beinahe stündlich. Doch trotz der vielen Aktualisierungen kann ein Antivirenprogramm nie alles entdecken – es braucht die Sensibilisierung der Benutzerinnen und Benutzer, um sich vor den Gefahren im Internet zu schützen.

Malware (die Abkürzung für Malicious Software, schädliche Software) ist ein Sammelbegriff für verschiedene Schadprogramme, die den PC befallen können. Es gibt eine Vielzahl von Unterarten: zum Beispiel Spyware, Trojanische Pferde, Viren, Würmer, Rootkits oder die im Moment stark grassierende Ransomware. Sie arbeiten zwar alle auf unterschiedliche Art und Weise, haben jedoch alle ein gemeinsames Ziel: Die Schädigung des Computers oder der Versuch viel Geld zu verdienen. Doch es gibt Massnahmen, um den eigenen PC oder Mac wirksam zu schützen.

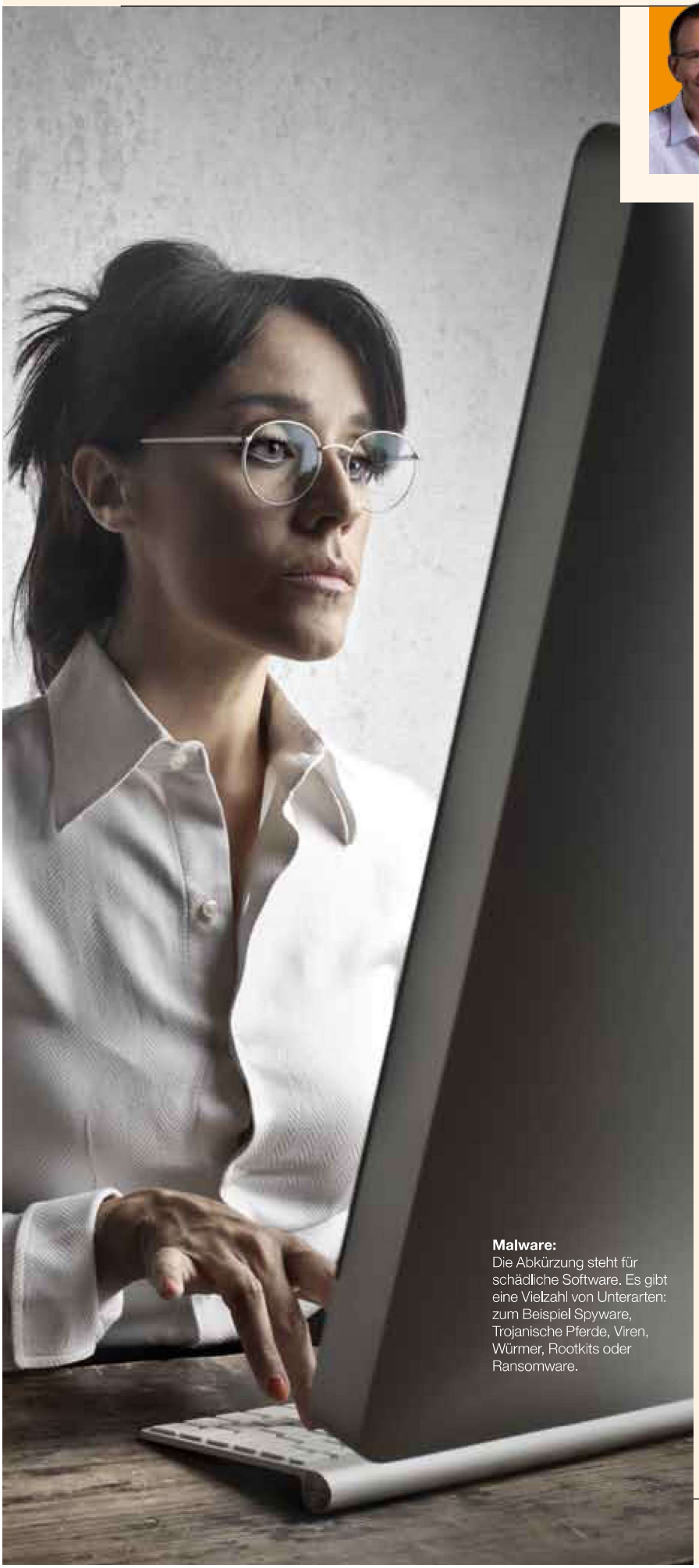
Wege für ein sicheres Surfen im Internet

Malware kann auf verschiedenen Wegen den eigenen Rechner befallen. Oftmals wird dies gar nicht bemerkt, wenn das Gerät befallen wird, sondern erst, wenn schon ein beträchtlicher Schaden entstanden ist oder gar nichts mehr geht. Es gibt glücklicherweise verschiedene Massnahmen, welche die Gefahr, Opfer einer Malware zu werden, stark reduzieren. Zu diesen Massnahmen zählen zum Beispiel:

- **Regelmässige Updates des Betriebssystems und der vorhandenen Applikationen**
  Die Betriebssysteme und Applikationen werden ständig weiterentwickelt, da oftmals erst nach der Veröffentlichung Sicherheitslücken und Fehler erkannt werden. Der Hersteller bietet daher in regelmässigen Abständen (meist) kostenfrei Verbesserungen des Systems, sogenannte Updates oder Patches, an. Updates können entweder manuell durch den Nutzer oder teilweise auch automatisch installiert werden. Da Sicherheitslücken heute im Internet gegen viel Geld versteigert werden, ist es wichtig, sehr schnell nach der Veröffentlichung einer Aktualisierung diese auch einzuspielen. Dies setzt die Hürde für einen erfolgreichen Angriff auf die eigenen Daten bereits massiv höher.

- **Antivirenprogramm nutzen und aktuell halten**
  Ein Antivirenprogramm schützt den eigenen Computer vor unerwünschter Malware, wenn es eine gute Qualität hat und stets auf dem Laufenden gehalten wird. Im

FOTOS: FOTOLIA UND ZVG



Malware:
Die Abkürzung steht für schädliche Software. Es gibt eine Vielzahl von Unterarten: zum Beispiel Spyware, Trojanische Pferde, Viren, Würmer, Rootkits oder Ransomware.

Andreas Wisler ist Dipl. Ing. FH, CISSP, CISA, ISO 22301 und 27001 Lead Auditor. Bei der goSecurity GmbH ist er als Senior IT-Security Auditor tätig (Penetration Tests, hersteller- und produkteneutrale Sicherheitsberatungen, ISO 27001 Zertifizierungsbegleitungen sowie Schulungen rund um die IT-Sicherheit).

Internet sind verschiedene Antivirenprogramme durch unabhängige Tests auf Herz und Nieren überprüft worden. Eine generelle Aussage, welches nun der beste Scanner ist, kann aber nicht getroffen werden. Zu verschieden sind die Funktionsweisen, mal schneidet das eine Programm besser ab, beim nächsten Test ein anderes. Viel wichtiger ist es daher, eines zu haben und dieses stetig zu aktualisieren.

- **Spamfilter des Providers oder der Antivirensuite nutzen**
  Spamfilter versuchen das eigene E-Mail-Postfach von lästigen Werbungen sauber zu halten und verhindern so manch eine Malware, die sich in einer Werbung oder in einem gut formulierten Bewerbungsschreiben versteckt sowie E-Mails von unbekannter Herkunft, die sich so auf den eigenen Rechner schleichen möchte. Aber auch hier gilt: es gibt keinen hundertprozentigen Schutz. Es benötigt immer noch den Menschen, der das letzte Urteil über die Seriosität des E-Mails fällt.

- **Mit Standardkonto ohne Administratorenrechte arbeiten**
  Wird der eigene Rechner von einem Virus befallen, übernimmt er die Rechte des aktuellen Benutzers und versucht sich tief ins System einzugraben und zu verstecken. Bei der alltäglichen Arbeit sollte daher ohne administrative Rechte gearbeitet werden. Benötigt ein Programm erhöhte Rechte, steht ein zweiter Account dafür zur Verfügung. Für moderne Betriebssysteme ist der duale Betrieb kein Problem mehr, in diesem Falle fragt das Betriebssystem vor jeder Änderung an den Daten nach dem entsprechenden Benutzer und Kennwort.

- **Gesunder Menschenverstand**
  Malware ist nicht leicht zu erkennen. Immer perfider werden die Angriffe. Sie verstecken sich oft in Benachrichtigungen, Bewerbungen oder zum Beispiel Wettbe-

werben und werden durch das Anklicken aktiviert. Bevor eine E-Mail geöffnet wird, sollte man sich überlegen, ob dies überhaupt relevant ist: «Erwarte ich ein Paket von DHL?» oder «Habe ich mein Konto bei dieser Bank?» E-Mails und Links sollten nur geöffnet werden, wenn sicher ist, dass etwas erwartet wird.

- **Jeden Link überprüfen**
  Oftmals verbirgt sich auch hinter einzelnen Links eine Malware. Dabei werden Schwachstellen in Browsern ausgenutzt, so kann sich bereits durch das reine Betrachten einer Website ein Schädling einnisten. Auch hier helfen ein gesundes Misstrauen und die Kontrolle, ob der Link auch wirklich dorthin führt, wie es angezeigt wird. Hilfreich ist dabei die Link-Scanning-Software URLVoid (www.urlvoid.com). Die Verwendung ist kostenfrei und die Kontrolle schnell erledigt. Auch Plugins wie WoT (Web of Trust) zeigen bereits auf allen Homepages sowie in Suchresultaten an, ob ein Besuch der Webseite gefährlich sein könnte.

- **Skriptblocker einsetzen**
  Bei jedem Besuch im Internet werden von den einzelnen Webseiten personenbezogene Daten über persönliche oder sachliche Verhältnisse gesammelt und gespeichert. Anschliessend kann der jeweilige Betreiber passende Werbung, die sich auf die gesammelten Daten beziehen, anzeigen. Dabei kann es sich zum Beispiel um die bevorzugten Einkäufe, Hobbys oder andere Vorlieben handeln. Durch Plugins wie Ghostery kann das Sammeln der sensitiven Daten auf fremden Servern massiv unterdrückt werden.

- **Fortwährend auf dem Laufenden bleiben**
  Nicht nur die Software entwickelt sich immer weiter. Die Hacker liefern sich ein regelrechtes Rennen mit den Entwicklern von Software und Antivirenprogrammen und versuchen immer wieder, die Schutzmechanismen der Computer zu unterwandern. Nur wer sich ausreichend informiert, weiss, worin die Gefahren der neuesten Malware bestehen und kann so den Gefahren entgegenwirken. Sicherheitshinweise auf Fachseiten und in Fachzeitschriften helfen, den Überblick zu bewahren. Wer immer auf dem Laufenden bleiben möchte, kann auch Newsletter abonnieren (zum Beispiel «BSI für Bürger» aus Deutschland oder «Melani» aus der Schweiz).

- **Backup der eigenen Daten**
  Das Erstellen von regelmässigen Backups ist die Lebensversicherung. Damit werden die Daten vor schädlichere Malware oder Diebstahl sowie bei Schäden des Gerätes geschützt. Da Verschlüsselungsviren (Ransomware) auch auf verbundene Netzlaufwerke zugreifen, müssen die Daten getrennt vom eigentlichen Betriebssystem aufbewahrt werden. Dies kann zum Beispiel auf einer externen Festplatte oder einem grossen USB-Stick erfolgen. Sollten die Daten aus irgendwelchen Gründen irgendwann doch einmal verloren gehen, so können diese durch die Kopie wieder auf den Stand gebracht werden, an dem das letzte Backup erfolgte.

- **Keine persönlichen Daten angeben**
  Praktisch überall wird nach der E-Mail oder weiteren (persönlichen) Informationen gefragt. Gerade im Bereich von Social Media, aber auch auf beliebigen anderen Webseiten, sollten Angaben zur eigenen Person nur mit grosser Vorsicht eingegeben werden. Es empfiehlt sich beispielsweise einen zweiten Account bei einem Freemailer oder einen Account, der nur einmal verwendet wird und mit einer extra dafür eingerichteten Web-Adresse versehen ist, zu benutzen. Wird eine Webseite einmal von einem Hacker gekapert, fallen die Daten nicht in die falschen Hände und das persönliche Postfach wird nicht mit Malware überschwemmt.

Diese zehn Punkte helfen mit, dass auch in Zukunft ein sicherer und virenfreier Umgang mit dem Internet möglich ist. Die Hürde für einen erfolgreichen Angriff wird damit sehr hoch angesetzt. Solange es einfachere Ziele gibt, bevorzugen Hacker diese und der Fokus wird auf andere gerichtet. ●

«Krisen gefährden den guten Ruf oder die Existenz.»