Andreas Hein

ABZOCKE IM INTERNET? NICHT MIT MIR!

SCHNELLEINSTIEG SICHER SURFEN IM WEB

160 SEITEN

ZEIGEN SIE POTENZIELLEN BETRÜGERN, WER AUF IHREM RECHNER DAS SAGEN HAT

FRANZIS

Andreas Hein

Schnelleinstieg
Sicher surfen im Web

Andreas Hein

SCHNELLEINSTIEG SICHER SURFEN IM WEB

FRANZIS

Bibliografische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte Daten sind im Internet über http://dnb.ddb.de abrufbar.

Herausgeber: Ulrich Dorn
Layout & Satz: Nelli Ferderer, nelli@ferderer.de
art & design: www.ideehoch2.de
Druck: CPI-Books
Printed in Germany

ISBN 978-3-645-60397-3

INHALT

1 GEFAHREN IM INTERNET

Das Internet ist zu einem ganz selbstverständlichen Teil des Alltags geworden, sodass sich viele Internetnutzer kaum noch ernsthafte Gedanken über die möglichen Gefahren machen, die dort lauern. Umso größer ist jedoch die böse Überraschung, wenn sie Opfer von kriminellen Aktivitäten werden. Weil das Internet längst nicht mehr nur zur Informationsbeschaffung, zum Spielen oder zur Kommunikation genutzt wird, sondern dort auch vermehrt kommerzielle Aktivitäten stattfinden und mit Onlinebanking und Onlineshopping finanzielle Transaktionen abgewickelt werden, wollen sich immer mehr Betrüger auf diesem Wege bereichern.

1.1 Gefahrenlage im Wandel

In den letzten Jahren hat das Sicherheitsbewusstsein bei vielen Internetnutzern überraschenderweise abgenommen, was auch darauf zurückzuführen ist, dass große, spektakuläre Angriffswellen durch Schadprogramme nicht mehr so häufig vorkommen und bekannt werden. Computerviren und Würmer, die weltweit Millionen von PCs befallen und lahmlegen, wie es Melissa und dem I-Love-You-Virus (auch Loveletter genannt) vor 15 Jahren gelang, gibt es heute nicht mehr. Das darf jedoch keineswegs als Entwarnung verstanden werden – ganz im Gegenteil! Es gibt neue Gefahren, die sogar noch gravierendere Folgen haben können.

Moderne Betriebssysteme und Rechner sind zwar tendenziell sicherer geworden, aber es gibt immer noch zahlreiche Schwachstellen, durch die sich Schadprogramme einschleichen können. Doch anders als vor 10 oder 15 Jahren zielen sie zumeist nicht mehr auf eine einfache Sabotage der Rechner oder haben das Ziel, undifferenziert möglichst viele PCs lahmzulegen. Perfiderweise versuchen viele neue Schädlinge, möglichst lange unentdeckt zu bleiben, um so ihren eigentlichen Zweck zu erfüllen. Sie spionieren den Nutzer und dessen Daten aus, um sich später beispielsweise beim Onlinebanking auf Kosten des Opfers zu bereichern, den Rechner fernzusteuern oder andere Manipulationen vorzunehmen. Die Betroffenen werden dabei direkt oder indirekt geschädigt, häufig werden auch ganz konkrete finanzielle Schäden angerichtet.

Handfeste Ziele

Die Amateurhacker der früheren Jahre entwickelten Computerviren, um damit ihr »Können« zu beweisen und ihre Fähigkeiten öffentlich zur Schau zu stellen. Heute werden Schadprogramme professionell entwickelt, und die Computer- und Internetkriminalität ist längst zu einem milliardenschweren Bereich der organisierten Kriminalität geworden.

Mit der neuen Schadsoftware verfolgen Angreifer ganz handfeste Ziele. Bei Angriffen auf Unternehmen werden Daten ausspioniert oder Rechner gezielt sabotiert. Werden Privatanwender nicht direkt finanziell geschädigt, missbrauchen Angreifer deren Rechnerressourcen für ihre Zwecke, indem sie die Kontrolle über die PCs übernehmen und diese fernsteuern. Von den folgenden Schadprogrammen und Angriffszenarien gehen derzeit die größten Gefahren aus.

Ransomware

Als Ransomware bezeichnet man Schadprogramme, die auf dem infizierten Rechner gezielt Dateien verschlüsseln, sodass kein Zugriff darauf mehr möglich ist. Erst nach Zahlung eines Lösegelds versprechen die Angreifer die Übersendung eines Freigabecodes, mit dem die Verschlüsselung wieder aufgehoben werden kann. Manchmal macht Ransomware die Nutzung eines PCs auch komplett unmöglich. Nach dem Einschalten des Rechners erscheint nur noch der Hinweis auf die Sperrung sowie eine Anleitung zur Zahlung des Lösegelds.

DER ERPRESSUNG NACHZUGEBEN BRINGT NICHTS

Wer der Erpressung nachgibt, wird nach der Zahlung des Lösegelds meist bitter enttäuscht, da das versprochene Passwort oder Tool zum Entschlüsseln des Rechners nicht geliefert wird. Der Schaden lässt sich trotz Zahlung nicht beheben. Manchmal bluffen die Erpresser aber auch nur, und die Blockade lässt sich mit ein paar Befehlen leicht aufheben. Tipps und Lösungen zu Ransomware-Angriffen finden Sie im Internet, das Sie dann mit einem nicht infizierten Rechner nutzen müssen.

Ein prominentes Beispiel für Ransomware ist der BKA-Trojaner. Dieser tarnt sich als Mitteilung der Bundespolizei und behauptet, dass auf dem Rechner verbotenes Material entdeckt worden sei. Es erscheint eine entsprechende Mitteilung mit der Aufforderung, einen bestimmten Betrag als Strafzahlung zu leisten.

Um der Forderung Nachdruck zu verleihen, wird der Rechner eingefroren und kann zunächst nicht weiter genutzt werden.

Der BKA-Trojaner war so erfolgreich, dass es mittlerweile zahlreiche Varianten davon gibt. Dieser Schädling kann zwar mit recht einfachen Mitteln deaktiviert werden, sodass eine normale Nutzung des Rechners schnell wieder möglich ist, es gibt aber auch deutlich gefährlichere Ransomware, die sich nicht so leicht abschalten lässt, sodass verschlüsselte Dateien nicht mehr zugänglich sind oder der Rechner nur durch eine komplette Neuinstallation des Betriebssystems wieder nutzbar wird.

Ransomware kommt immer öfter zum Einsatz.

Botnetze und Zombie-Rechner

Zu einem Missbrauch, von dem die Opfer häufig gar nichts oder nur indirekt etwas mitbekommen, kommt es, wenn Rechner durch eine Fernsteuerungssoftware befallen werden. Angreifer bekommen dadurch die Möglichkeit, den Rechner und seine Ressourcen für ihre Zwecke zu verwenden, indem sie einfach entsprechende Befehle übermitteln. Die manipulierten Rechner werden als Zombie-PCs oder einfach als Zombies bezeichnet. Besonders erfolgreiche

Schädlinge dieser Art haben weltweit Millionen von PCs befallen, die wie ein Heer willenloser Sklaven die Befehle ihrer Herren ausführen. Eine solche Ansammlung ferngesteuerter Rechner wird Botnet (oder eingedeutscht Botnetz) genannt.

Ist ein solches Botnetz eingerichtet, nutzen die Betreiber es meistens nicht selbst, sondern vermieten die enormen Ressourcen an andere Interessenten. Häufig wird über diese Netze unerwünschte E-Mail-Werbung (Spam) versendet. Die Rechner werden aber auch missbraucht, um sogenannte DDOS-Angriffe (*Distributed Denial Of Service*) auf Internetserver durchzuführen, die durch massenhafte gleichzeitige Aufrufe durch die ferngesteuerten PCs gezielt überlastet und für andere Besucher unerreichbar gemacht werden. Mit DDOS-Angriffen werden Webshops und andere kommerzielle Internetanbieter bedroht, die durch das Lahmlegen ihrer Server erhebliche Einbußen hätten. Oft kommen zunächst nur kurze Angriffe, um anschließend Schutzgelder von den Betreibern zu erpressen, die häufig lieber zahlen, als weitere Attacken dieser Art hinzunehmen oder teure Schutzvorkehrungen zu installieren.

Als Besitzer eines PCs, der durch eine Schadsoftware infiziert und Teil eines Botnetzes ist, bekommen Sie jedoch meist nicht mit, dass Ihr Rechner für derartige Machenschaften missbraucht wird, und sind völlig ahnungslos. Einige Provider informieren daher ihre Kunden, wenn sie verdächtige Aktivitäten an deren Internetzugängen feststellen.

HILFE BEIM BOTNET-BERATUNGSZENTRUM

Haben Sie den Verdacht, dass Ihr Rechner Teil eines Botnetzes ist, können Sie sich auf der Website des Anti-Botnet-Beratungszentrums darüber informieren, wie Sie diese Schadsoftware wieder entfernen und sich vor derartigen Übergriffen künftig schützen können. Die Seite erreichen Sie unter der Adresse *www.botfrei.de*.

Betrügereien beim Onlinebanking

Besonders im Fokus der Betrüger stehen natürlich Anwender, die ihre Geldgeschäfte via Onlinebanking tätigen, denn hier machen sich Betrügereien direkt in klingender Münze bezahlt. Bereits seit geraumer Zeit findet ein Wettlauf

8 DATENSICHERHEIT IN SOZIALEN NETZWERKEN

Noch mehr als Clouddienste haben in den letzten Jahren soziale Netzwerke die Internetnutzung revolutioniert. Seit Dienste wie Facebook, Twitter und Instagram ihren unaufhaltsamen Siegeszug angetreten haben, kennen viele Menschen kein Halten mehr, wenn es darum geht, auf die Schnelle ihre Meinungen, Kommentare und Fotos zu veröffentlichen. Doch nicht immer sind sie sich der Folgen ihres Tuns bewusst, denn einmal in der Öffentlichkeit der sozialen Netze präsentiert, lassen sich Inhalte nicht einfach wieder entfernen, selbst wenn man das möchte. Wenn Sie mit persönlichen Informationen nicht allzu freigiebig sein möchten, müssen Sie auf Facebook & Co. zwar nicht komplett verzichten, sollten aber einiges bei der Nutzung beachten.

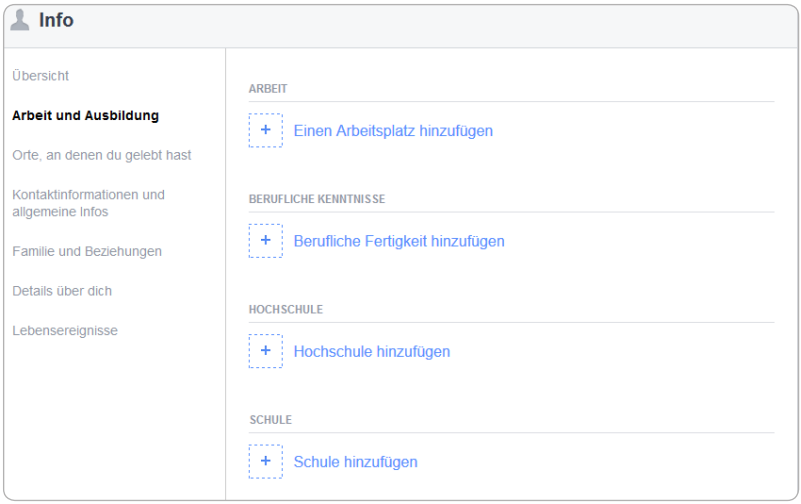
8.1 Wer sollte was wissen dürfen?

Ohne ständigen Zugriff auf soziale Netzwerke scheinen viele Mitmenschen kaum noch leben zu können. Neuigkeiten werden mit der immer größer werdenden Schar von »Freunden« ausgetauscht und kommentiert, man trifft sich auf Twitter und lästert hier über den gerade laufenden Fernsehkrimi ab, äußert seine Betroffenheit über die Naturkatastrophe am anderen Ende der Welt oder verabredet sich zwecks gemeinsamer Freizeitgestaltung.

Schon bei der Anmeldung geben bei den meisten Diensten die Nutzer viel von sich preis, wenn sie neben ihrem Namen und den Kontaktdaten noch Informationen zu schulischem und beruflichem Werdegang in ihre Profile eintragen, ihre Hobbys und Lieblingsbücher bzw. Filme benennen und ähnliche Angaben machen. Einerseits stellen diese Informationen die Grundlage der sozialen Netzwerke dar, denn man will ja schließlich mit alten oder neuen Freunden und Bekannten in Kontakt treten, andererseits veröffentlicht man damit auch Informationen, die man im realen Leben aus gutem Grund längst nicht jedem Unbekannten einfach so mitteilen würde.

Auch bei der alltäglichen Nutzung der Dienste kann es leicht problematisch werden. Unter Umständen lässt man sich aus einer Laune heraus zu einem missverständlichen Kommentar hinreißen oder verfasst eine Mitteilung, die man mit etwas Abstand im Nachhinein bereut. Zwar können Sie Bilder, Postings und Kommentare nachträglich wieder löschen, doch wenn sie bereits für Aufsehen gesorgt haben und im Freundeskreis oder gar darüber hinaus diskutiert werden, lässt sich die Tatsache, dass diese Meldungen einmal online waren, nicht mehr leugnen. Denn Bilder und Meldungen können jederzeit einfach

kopiert werden und sind damit auch nach dem Löschen des Originalbeitrags weiter verfügbar. Dass die Redewendung vom Internet, das nichts vergisst, durchaus keine weltfremde Floskel, sondern bittere Realität ist, haben schon viele Nutzer erfahren müssen.



Soziale Netzwerke sind an Informationen aus allen Lebensbereichen interessiert.

AUCH PERSONALABTEILUNGEN KENNEN FACEBOOK

Wenn Sie sich auf Facebook oder anderen sozialen Netzwerken öffentlich in Szene setzen, müssen Sie bedenken, dass diese Informationen auch Personen zugänglich sind, an die Sie zunächst gar nicht denken. So informieren sich immer öfter auch potenzielle Arbeitgeber über Stellenbewerber via Facebook, und nicht immer fällt das Fazit nach der Betrachtung der Chroniken positiv aus.

Nicht nur bei Bewerbungen können Facebook-Aktivitäten Folgen haben, auch in anderen Situationen werden die öffentlich zugänglichen Informationen vielleicht zu einem Nachteil:

- Arbeitnehmer können eine Abmahnung erhalten, wenn sie sich negativ über ihren Arbeitgeber geäußert haben.
- Schüler müssen mit Konsequenzen rechnen, wenn sie sich beleidigend über Lehrer oder Mitschüler äußern.
- Vermieter können eine Facebook-Recherche nutzen, um Mieter mit unerwünschten Eigenschaften und Aktivitäten zu identifizieren.
- Versicherungen können anhand der angegebenen Hobbys Kunden mit besonderen Risiken identifizieren und Angebote einschränken oder höhere Tarife fordern.
- Letztlich können auch Onlinebetrüger über das Sammeln persönlicher Daten in den Netzwerken Informationen gewinnen, die sie anschließend für das Social Engineering einsetzen, um maßgeschneiderte Phishing-Angriffe zu starten.

Bei der Nutzung sozialer Netzwerke gibt es zwei Aspekte im Hinblick auf Datenschutz. Zum einen geht es wie in den eben beschriebenen Fällen um die Daten, die Sie freiwillig veröffentlichen, und darum, wie diese von anderen Nutzern wahrgenommen werden oder was andere Nutzer mit diesen Informationen anfangen. Der andere Aspekt ist die Datensammlung der sozialen Netzwerke selbst. Diese erfassen Ihre Aktivitäten genau und nutzen diese Daten für eigene Zwecke. Da die meisten sozialen Netzwerke kostenfrei nutzbar sind und das nach eigenem Bekunden auch so bleiben soll, müssen sie sich ja auf andere Weise finanzieren. Die wichtigste Einnahmequelle ist die Werbung, und für Werbetreibende ist es wiederum sehr wichtig, dass ihre Werbemittel möglichst ohne Streuungsverluste genau bei der Zielgruppe ankommen. Je besser ein soziales Netzwerk Sie kennt und über Ihre Vorlieben und Gewohnheiten Bescheid weiß, desto wertvoller sind Sie für den Betreiber, denn diese Informationen kann es an die Werbetreibenden weiterverkaufen.

Grundlegende Regeln für den Umgang mit sozialen Netzwerken

Die Nutzung sozialer Netzwerke setzt natürlich voraus, dass Sie bereit sind, Informationen über sich bereitzustellen, und über Ihre Profile und Kontaktdaten für andere erreichbar und auffindbar sind. Dennoch sollten Sie nicht zu freigiebig sein und das Prinzip der Datensparsamkeit anwenden, also immer nur so viele Daten preisgeben, wie wirklich benötigt werden.

ECHTER NAME ODER PSEUDONYM?

Die Frage der Datensparsamkeit betrifft auch die grundlegende Entscheidung, ob Sie ein Konto in einem sozialen Netzwerk unter Ihrem richtigen Namen eröffnen möchten oder ob der Auftritt unter einem Pseudonym oder Spitznamen erfolgen soll. Prinzipiell sieht der Gesetzgeber im Telemediengesetz vor, dass eine Nutzung auch unter Pseudonym möglich sein soll, allerdings verlangt Facebook die Verwendung des echten Namens und behält sich bei Verstößen gegen diese Vorgabe vor, das Konto zu sperren. Rechtlich gibt es hier noch Klärungsbedarf, und es bleibt abzuwarten, wie über derartige Streitfälle entschieden wird.

Bei zweckgebundenen sozialen Netzwerken, etwa einem primär für berufliche Zwecke genutzten Netz wie etwa Xing, ergibt es keinen Sinn, ein Profil unter einem Pseudonym einzurichten, hier ist die Verwendung des echten Namens angeraten.

Bei der Anmeldung bei einem sozialen Netzwerk werden Sie zu einer möglichst umfassenden Angabe von Profildaten aufgefordert. Hierzu gehören auch Angaben zu Schulausbildung, Religionszugehörigkeit, politischen Ansichten, Familienstand und vielem mehr. Sie sollten sich immer genau überlegen, welche Informationen Sie mitteilen wollen und welche davon allen anderen Nutzern des Netzwerks angezeigt werden sollen. Mitunter ist es möglich, bestimmte Inhalte allgemein freizugeben und andere Profildaten dagegen nur ausgewählten Nutzern zugänglich zu machen.

Religiöse und politische Ansichten sollten Sie eher nicht veröffentlichen.

Die meisten sozialen Netzwerke ermöglichen es, verschiedenen Nutzergruppen unterschiedlichen Zugriff auf die eigenen Daten einzuräumen. Mitunter wird dabei nur zwischen allen Nutzern des Diensts (bzw. sogar allen Internetnutzern) und der Gruppe der Freunde unterschieden. Häufig gibt es auch

weitere Unterteilungen, etwa in Familie oder enge Freunde. Vor allem bei den Einstellungen zur Freigabe von Daten für die Gesamtheit der Nutzer sollten Sie nach Möglichkeit restriktiv vorgehen und nur die notwendigsten Angaben allgemein zugänglich machen.

WEITERE KONTAKTDATEN BESSER NICHT ANGEBEN

Abzuraten ist von der Weitergabe zusätzlicher Kontaktdaten. Soziale Netzwerke ermöglichen bereits die Erreichbarkeit über die interne Kommunikationsplattform und/oder die E-Mail-Adresse. Postanschrift und Telefonnummer sollten Sie nach Möglichkeit nicht mitteilen.

Auch die Veröffentlichung Ihrer Freundesliste können Sie bei vielen sozialen Netzwerken beschränken. Das kann durchaus sinnvoll sein, denn allein schon aus diesen Kontakten können andere Rückschlüsse auf Ihre Person ziehen.

SPERREN SIE SUCHMASCHINEN AUS

Kontrollieren Sie, ob das soziale Netzwerk die von Ihnen angegebenen persönlichen Daten nur anderen Nutzern des Netzwerks anzeigt oder ob diese Angaben auch Suchmaschinen zugänglich gemacht werden. Bei einigen sozialen Netzwerken können Sie in den Einstellungen festlegen, dass die eigenen Daten für Suchhilfen nicht zugänglich gemacht werden sollen.

In vielen sozialen Netzwerken gibt es Anwendungen von Drittanbietern, mit denen zusätzliche Funktionen nutzbar sind. Oftmals wollen diese Anwendungen auf Ihre Profildaten zugreifen, wobei die Informationen aus diesen Zugriffen häufig auch für unerwünschte Zwecke wie Werbung genutzt werden. Sie sollten daher bei Verwendung derartiger Anwendungen genau darauf achten, ob diese einen Zugriff auf die Profildaten verlangen, und sich genau überlegen, ob Sie das tatsächlich auch zulassen wollen.

INDEX

Symbole

A

B

C

W

X

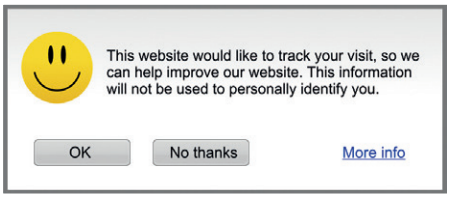
Z

SCHNELLEINSTIEG
SICHER SURFEN IM WEB

ABZOCKE IM INTERNET? NICHT MIT MIR!

„Checklisten und Sicherheitstipps – entspannt Surfen“

Computerviren und Würmer, die weltweit Millionen von PCs befallen und lahmlegen, wie es Melissa und dem I-Love-You-Virus vor 15 Jahren gelang, gibt es heute nicht mehr. Das darf jedoch keineswegs als Entwarnung verstanden werden – ganz im Gegenteil! Es gibt neue Gefahren, die sogar noch gravierendere Folgen haben können.



Erprobte Sicherheitskonzepte für entspanntes Surfen, am Beispiel realer Betrügereien vorgestellt
(Quelle: Screenshots silktide.com, paypal.de)

Lassen Sie sich den Spaß am Internet nicht verderben ...
Auch wenn die Aufzählung der potenziellen Gefahren auf den ersten Blick recht abschreckend wirkt, müssen Sie nicht gleich in Panik geraten und auf die Internetnutzung verzichten. Zum Glück gibt es zahlreiche Möglichkeiten, die Risiken so weit zu verringern, dass Sie sich weiterhin weitgehend unbeschwert im Internet bewegen und von den vielfältigen Nutzungsmöglichkeiten profitieren können.

... werden Sie aktiv, handeln Sie und geben Sie Betrügern keine Chance
Dieses Buch ist Ihr Schild gegen Botnetzte und Zombie-Rechner, gegen Betrügereien beim Onlinebanking, gegen Identitätsdiebstahl, gegen unerwünschte Überwachung und Datenweitergabe – Ihr Schild gegen den alltäglichen Betrug. Sicherheit beim Surfen stellt sich nicht von allein ein. Sie müssen selbst aktiv werden! Dabei ist es nicht mit einer einmaligen Aktion wie der Installation eines Antivirenprogramms getan, sondern Sie sind dauerhaft gefordert, aufmerksam zu bleiben und vorsichtig zu handeln. Dieses Buch hilft Ihnen dabei.

Aus dem Inhalt:

9 783645 603973