Ad- und Spyware

# Gefährliche Schnüffler im Netz

**Sie wundern sich, wie Unternehmen an Ihre persönlichen, auf Ihrem Computer gespeicherten Informationen gelangen? Die Sicherheitsrisiken im Internet manifestieren sich auf vielfältige Weise. Ob Viren, Würmer, Ad- oder Spyware – lästig sind die Schädlinge alle. Wie Unkraut verwurzeln sie sich in unseren Systemen und sind oft nur sehr schwer loszuwerden. Durch den Einsatz von Spyware profitieren am Ende die Hersteller, welche ihre unrechtmässig erfassten Daten an Dritte weiterverkaufen können.**

**Kontakt:**

**Reto Inversini**
BIT, Telekommunikation, Operative Sicherheit

**Redaktion: Boe**

Ändert sich die Startseite Ihres Browsers ohne ersichtlichen Grund oder öffnen sich Werbefenster, welche in keinem erkennbaren Zusammenhang mit der besuchten Webseite stehen? Gibt es Buchungen auf Ihrer Kreditkarte, die Sie sich nicht erklären können? Sind plötzlich Links unter Ihren Favoriten, welche Sie nicht gespeichert haben oder erhalten Sie häufig Werbemails von unbekannten Absendern? Dann könnte es sein, dass Sie ausspioniert werden. Die so genannte Spyware oder Spionagesoftware ist zwar zu einem Sicherheitsrisiko geworden, aber nicht jedes Programm hegt kriminelle Absichten. Mit den richtigen Massnahmen und Programmen sind die Anwender keineswegs machtlos.

## Malware

Software, welche Schaden anrichtet oder illegale Aktionen durchführt, wird unter dem Oberbegriff Malware zusammengefasst. Ihre Erscheinungsformen variieren ebenso wie ihre Angriffstechniken:

- **Viren** sind Programme, die sich selbst reproduzieren.
- **Würmer** verbreiten sich über Netzwerke ohne Interaktion des Users.
- **Trojanische Pferde** öffnen Hintertürchen zur Fernsteuerung von infizierten Computern.
- **Keylogger** schreiben die Tastatureingaben mit und können so beispielsweise an Kreditkartennummern oder Passwörter gelangen.
- **Ad- und Spyware** erstellt Benutzerprofile oder sammelt sensible Daten.

Die heutigen Ad- und Spyware-Angriffe sind ein ziemlich junges Phänomen. Die Grenze zwischen den beiden ist fliessend. Im Gegensatz zu Adware werden bei Angriffen durch Spyware Daten ohne explizites Wissen des Benutzers erfasst und analysiert. In der Schweiz ist ein solches Vorgehen strafbar. Durch die weltweit unterschiedlichen Gesetzgebungen betreffend Informatikdelikten kann jedoch ein bei uns verbotenes Programm in einem anderen Land völlig legal sein. Wenn gut organisierte Angreifer von Ländern aus operieren, die eine ungenügende Gesetzgebung haben, sind sie auch für die Strafverfolgung aus der Schweiz praktisch unangreifbar.

## Interessen der Angreifer

Das Schreiben von Malware wurde professionalisiert. Dementsprechend geht es auch um viel Geld. Die vereinzelten Technikfreaks, welche Malware programmieren, fallen heute im Gegensatz zu grösseren kriminellen Vereinigungen kaum mehr ins Gewicht. Die verbesserte Organisation und die hohe Arbeitsteilung innerhalb dieser Vereinigungen machen die Verfolgung äusserst schwierig. Adware wird von den Herstellern benutzt, um ihre Programme zu finanzieren. Wer sich an der Werbung stört, kann in der Regel gegen eine Gebühr eine werbefreie Software erstehen. Spyware hingegen lässt den Benutzen-

français

**Logiciels espion et publicitaires – De dangereux renifleurs sur le réseau**
Vous vous demandez comment des entreprises obtiennent vos informations personnelles, enregistrées sur votre ordinateur? Les risques en matière de sécurité sur Internet se manifestent de diverses manières. Qu'il s'agissent de virus, de vers, de logiciels espion ou publicitaires, ces parasites nuisibles sont tous agaçants. Ils s'enracinent dans nos systèmes comme de la mauvaise herbe, et il est souvent très difficile de s'en défaire. Somme toute, ce sont les constructeurs qui profitent des logiciels espion, en vendant des données saisies illégalement à des tiers.

Vous trouverez la version complète en français sur intranet à l'adresse:
http://www.bit.admin.ch/eisbrecher

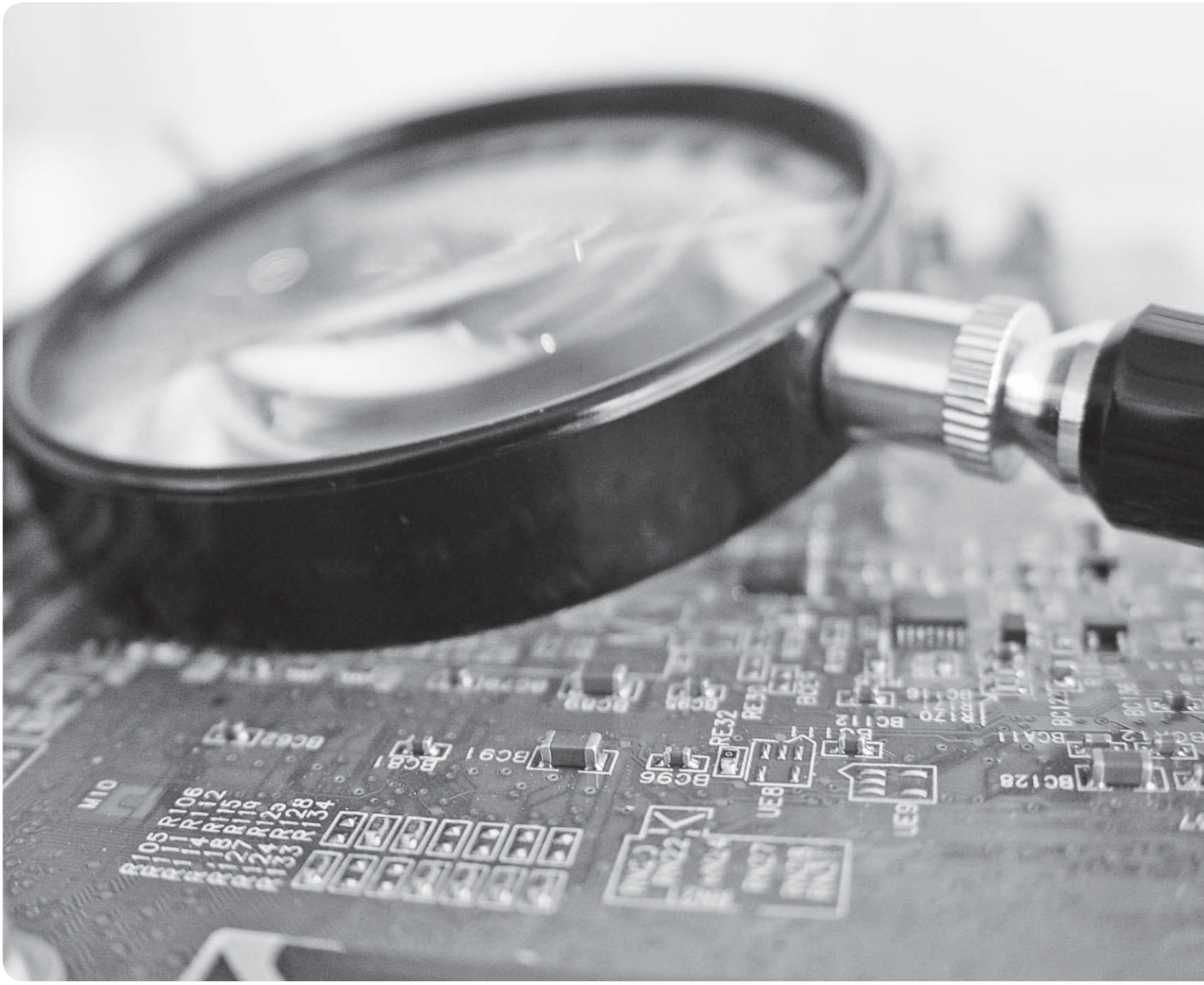
deutsch

den diese Wahl nicht. Ihr Surfverhalten wird vom Webbrowser auf der Festplatte dokumentiert (History, Cookies usw.) und – ohne dass Sie es merken – analysiert. Die so erstellten Profile sind ein lukratives Geschäft für deren Vermittler.

**Seien Sie misstrauisch**

Was für die einen ein Ärgernis ist, generiert für andere einen Nutzen. Die Grenzen zwischen praktischem Tool und Schädling sind nicht immer klar. Im Gegensatz zu Viren oder Würmern ist der Begriff Spyware bisher weniger eindeutig definiert. Nebst Spyware hat sich denn auch der Name PUP (potentially unwanted program) durchgesetzt. Ein ungewolltes Programm kann aus einem anderen Betrachtungswinkel durchaus erwünscht sein.

Sicherheit beginnt auch hier bei den Anwendern. Was können Sie gegen diese schädlichen Programme unternehmen? Bei kostenloser Software ist grundsätzlich Vorsicht geboten. Schauen Sie sich die Websites genau an. Verdächtig ist zum Beispiel, wenn Sie keine Kontaktmöglichkeiten der betreffenden Firma finden. Bevor Sie Ihre definitive Zustimmung zu einem Download geben, schauen Sie sich auch das Kleingedruckte der Endnutzervereinbarungen an. Dort verstecken sich ab und zu Hinweise auf Ad- oder Spyware. Vorschnelles Akzeptieren kann eine Zustimmung zur Spionage bedeuten. Recherchieren Sie z. B. mit Google, ob andere Benutzer bereits schlechte Erfahrungen mit einem Programm gemacht haben oder ob bekannte Meldungen



*Spyware schleicht sich heimlich auf die Rechner und spioniert Nutzergewohnheiten und -daten aus.*

vorliegen, dass ein Programm mit Spyware gekoppelt ist.

Wenn Sie auf Ihrem Computer am Arbeitsplatz die Berchtigung haben, selbstständig Software zu installieren, sind Sie auch verantwortlich dafür, dass diese Programme keine Spyware enthalten. Zudem müssen Sie darum besorgt sein, dass Sie es erfahren, wenn bei einem selbst installierten Programm eine Sicherheitslücke auftaucht. In diesem Fall müssen Sie auch den notwendigen Patch einspielen.

Seien Sie misstrauisch, wenn Sie ein Mail erhalten, welches Sie auffordert, auf einen Link zu klicken, um dort Ihre Account-Daten zu erneuern. Wenn Sie Online Banking betreiben, geben Sie die URL zum Server der Bank immer von Hand ein und klicken Sie nie direkt auf einen Link in einem Mail.

Deaktivieren Sie die HTML-Ansicht in Ihrem E-Mail-Programm. Dies mindert diverse Gefahrenquellen. Die meisten E-Mail-Programme erlauben es zudem, das Nachladen von Grafiken aus dem Internet zu unterbinden.

Speichern Sie keine sensitiven Informationen wie Passwörter unverschlüsselt auf Ihrem Computer.

**Infobox:**

- **Adware** sind Programme, welche unerwünschte Werbebanner anzeigen. Die Hersteller nutzen Adware, um die kostenlosen Versionen ihrer Programme zu finanzieren.
- **Spyware** ist Software, die ohne Wissen des Benutzers auf dessen Computer gelangt, Daten sammelt und diese unbemerkt versendet. Spyware tarnt sich oft in harmloser Free- oder Shareware oder nützt gar Lücken im Webbrowser aus, um sich unbemerkt auf einem System zu installieren.
- **Phishing** bezeichnet Aktionen, welche die Benutzenden dazu veranlassen, vertrauliche Informationen an die Angreifer weiterzugeben. Das Kunstwort setzt sich aus Password, Harvesting (Ernte) und Fishing zusammen.
- **Webbugs** sind kleine, unsichtbare Grafiken. Diese werden oft zur Informationsgewinnung eingesetzt. Die Betreiber können so beispielsweise feststellen, ob und von wo aus ein Spammail geöffnet wurde.
- **Pharming** bedeutet das Vergiften eines DNS-Servers, um die Benutzenden auf den Server des Angreifers umzuleiten. Diese Methode ist effizient, weil so eine grosse Anzahl potentieller Opfer erreicht wird.