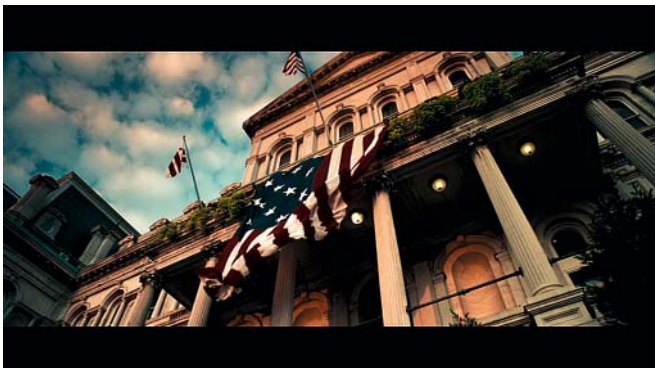
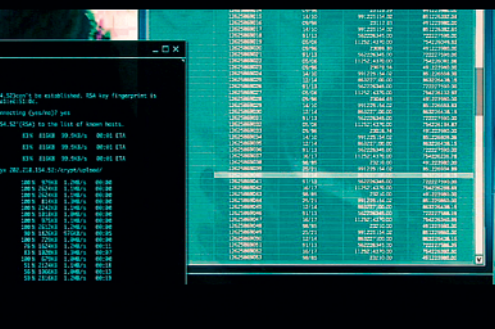


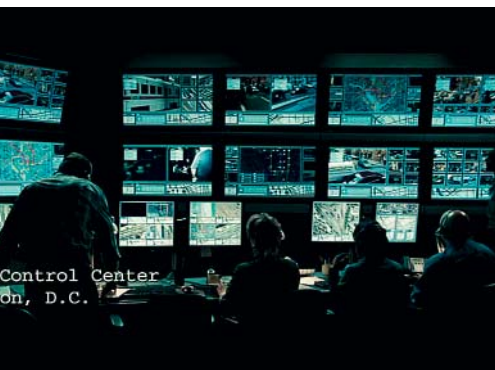
SICHER IST NUR DIE NÄCHSTE ATTACKE

Der jüngste Spionageangriff auf das EDA führt die Anfälligkeit von Computernetzen vor Augen. Die Cyber-Kriminalität nimmt zu, das Risiko steigt. Betroffen sind Regierungen ebenso wie Firmen.





In «Live Free or Die Hard», dem vierten Teil der erfolgreichen «Die Hard»-Filmserie, legt ein raffinierter Hacker die Computersysteme lahm und erpresst die US-Regierung.



► **CLAUDE SETTELE** TEXT

Am 26. Oktober meldete das Eidgenössische Departement für auswärtige Angelegenheiten (EDA), dass sich professionelle Hacker mittels einer speziellen Software Zugang zum Computernetz verschafft hätten, um gezielt Informationen zu beschaffen. Jetzt führt die Bundesanwaltschaft ein gerichtspolizeiliches Ermittlungsverfahren wegen Verdachts auf unbefugtes Eindringen in ein Datenverarbeitungssystem und verbotenen Nachrichtendienst. Laut Mediensprecherin Jeannette Balmer können zum jetzigen Zeitpunkt keine Einzelheiten bekanntgegeben werden.

Den meisten unter uns dürften solche Angriffe in erster Linie aus Kinofilmen wie «Live Free or Die Hard» mit Bruce Willis oder dem Robert-Redford-Klassiker «Sneakers» bekannt sein, aber sie sind auch im realen Leben keine Einzelfälle. Bereits vor zwei Jahren waren das EDA und das Staatssekretariat für Wirtschaft (Seco) Zielscheibe eines erfolgreichen Angriffs. Die kriminelle Energie der Hacker steigt, und sie dringen längst nicht mehr nur um des Ruhmes willen in ein Computernetzwerk ein, sondern im Auftrag gegen gutes Geld. Sie suchen ständig nach neuen Lücken und Tricks, um die Firewalls und Sicherheitsbollwerke zu löchern.

Auch andere Länder werden immer wieder Opfer von Hackeraktivitäten. Im Juli dieses Jahres wurde eine Angriffswelle gegen Websites in Südkorea und den USA registriert. Betroffen waren mehrere US-Ministerien wie auch Firmen, deren Websites aufgrund einer Denial-of-Service-Attacke (DoS; siehe «Glossar der Hacker» auf Seite 79) für mehrere Tage un erreichbar waren. Für Firmen, die übers Web Produkte verkaufen und Dienstleistungen anbieten, bringen solche Vorfälle nicht nur einen Imageschaden, sondern sind oft auch mit wirtschaftlichen Folgen verbunden. Fast glimpflich davon kam die Cablecom, als der Kabelnetzbetreiber Anfang Jahr Opfer einer DoS-Attacke wurde: Im Grossraum Zürich waren die Internet- und Telefondienste auf dem Cablecom-Netz kaum oder nicht mehr zu benutzen, wenn auch «nur» während knapp einer Stunde.

Selbst im Pentagon, dem Hochsicherheitstrakt des US-Verteidigungsministeriums, gibt es immer wieder Datenlecks. So tummelte sich ein britischer Hacker unbemerkt 13 Monate lang im Netz. Der Fall liegt schon sieben Jahre zurück und scheint von der harmloseren Sorte zu sein.

Der Hacker soll angeblich nur nach internen Berichten über Ufos gesucht haben. Als GAU bezeichnen kann man jedoch den zweiten Einbruch, den auch die verschärften Sicherheitsmassnahmen nicht verhindern konnten: Im April dieses Jahres meldete das «Wall Street Journal» in einem später von der Regierung bestätigten Bericht, Hacker hätten über mehrere Monate im Pentagon die Details zum geplanten neuen Kampffjet F-35 der US-Armee ausspioniert.

Nicht nur Regierungen werden immer wieder Opfer von kriminellen Hackern, sondern auch Firmen sind betroffen. Sie sprechen nicht gerne über die Bedrohungslage und schon gar nicht über allfällige Angriffe und deren Folgen. Verschwiegen gaben sich denn auch die Schweizer Unternehmen, die BILANZ nach ihren Erfahrungen befragte. Konkrete Antworten mochten weder ABB noch Novartis geben. In Fragen der Sicherheit lassen sich die Firmen nicht gern in die Bücher sehen.

BETRUG UND SPIONAGE. Will der Chief Security Officer eines Unternehmens gut schlafen, dann träumt er von seinem Computernetz als einem abgeschoteteten Bollwerk: Firewalls als Schutzwände, eine entmilitarisierte Zone, wie im Jargon des Cyberwar der Puffer zwischen Feind und Firma genannt wird.

Werkspionage ist so alt wie das Unternehmertum. Die Beschaffung von Informationen über Produkte und Forschungsergebnisse sowie Kunden- und Mitarbeiterdaten der Konkurrenz sind einige der Motive, Hacker für das Eindringen in Firmennetze zu bezahlen. Oftmals geht es auch nur darum, auf dem Mail-Server Adressen für potenzielle Spam-Empfänger zu beschaffen oder Malware (Schadprogramme) einzuschleusen, um die Rechner der Firma für ein Bot-Netz (weitgehend autonom tätige Computerprogramme) und einen Angriff auf Dritte zu missbrauchen.

Eher selten werden solche Vorkommnisse öffentlich gemacht, in vielen Fällen nehmen die betroffenen Firmen selbst auch gar keine Kenntnis davon.

Doch immer wieder verdeutlichen schwerwiegende Fälle von Firmen-Hacking das Risikopotenzial. So beispielsweise der Fall des US-Finanzdienstleisters Heartland Payment Systems. Die Firma, die monatlich 100 Millionen Kreditkarten- ►

Film-Stills: Twentieth Century Fox Film Corporation

SMARTPHONES

Risikofaktor Handy

Smartphones sind kleine Computer. Und als solchen drohen ihnen dieselben Gefahren wie den PC.

Smartphones sind nichts anderes als Mini-Computer mit drahtloser Internetverbindung. Sie sind also denselben Risiken ausgesetzt wie PC und damit ebenso anfällig für Viren, Würmer und Trojaner. Ist das Gerät nicht mit einer Antivirensoftware geschützt, besteht die Gefahr, dass zum Beispiel beim Synchronisieren schädigende Software ins PC-Netz eingeschleust wird. Handys können auch gehackt werden, wie die TV-Sendung «Kassensturz» jüngst zeigte: Ein Hacker übernahm die Kontrolle über das Handy eines Tele2-Kunden und versandte für über 20 000 Franken Massenmails.

Auch bei Verlust oder Diebstahl werden Handys mit geschäftskritischen Daten zum Risiko. Viele Unternehmen kennen deshalb unterschiedliche Richtlinien über die Nutzung und die Wahl der erlaubten Modelle, besonders für Kaderleute.

Auch die Abhörsicherheit ist ein Thema. Ein Fan des bei Managern beliebten BlackBerry ist Barack Obama. Nach seiner Wahl wollte ihm die National Security Agency den Einsatz des Geräts verbieten. Er intervenierte und bekam einen präparierten BlackBerry für den Privatgebrauch. Später entwickelte der Geheimdienst für den Präsidenten eine Verschlüsselung für geschäftliche Gespräche. Doch in Europa gibt es Unternehmen, die vom BlackBerry abrücken. Laut dem deutschen Magazin «Capital» will etwa die deutsche Autoindustrie künftig auf die Handys der kanadischen Firma Research In Motion (RIM) verzichten. Das Problem: Blackberrys setzen zwar auf starke Verschlüsselung, doch in Europa laufen alle Gespräche über einen RIM-Server in London. Befürchtet werden Spionage und ein Zugriff des britischen Geheimdienstes auf die Daten.



Von Ampelsteuerungen bis zu Überwachungskameras – alles ist computergesteuert und damit ein potenzielles Ziel für kriminelle Elemente.

► transaktionen für 175 000 Restaurants und Shops abwickelt, meldete Anfang Jahr, sie sei Opfer von Hackern geworden. Im bisher grössten Fall von Kreditkartenbetrug sind nun drei Hacker angeklagt, ein Amerikaner und zwei Russen. Sie haben sich während mehrerer Monate unbemerkt im Firmennetz von Heartland bewegt und die Daten von über 130 Millionen Kredit- und Debitkarten gestohlen. Diese verkauften sie im Internet und bedienten sich auf fremden Bankkonten.

In der Schweiz ermittelt die Bundesanwaltschaft bereits seit 2007 in mehreren Phishing-Fällen gegen Schweizer Finanzinstitute. In den Medien wurden UBS, CS und PostFinance als betroffene Firmen genannt, was die Bundesanwaltschaft auf Anfrage nicht bestätigen will. Die Untersuchungen laufen im Rahmen einer internationalen Justizkooperation und seien deshalb sehr aufwendig.

RISIKOFAKTOR MITARBEITER. Cyber-Kriminelle setzen zwar immer noch klassische Mittel wie Zero-Day-Attacks ein, ihre Taktik fokussiert aber zunehmend auch auf den Risikofaktor Mensch. Sie machen sich die Neugier und Spielfreude zunutze und locken Anwender auf Websites mit lustigen YouTube-Videos. Die Filmchen sind mit Trojanern infiziert. Oder sie nutzen News-Websites als getarnte Fallen und locken bei Ereignissen wie dem Tod Michael Jacksons Tausende von zu Hause und vom Büro an.

Immer noch öffnen viele Anwender unbekümmert Dateianhänge von E-Mails unbekannter Absender und können sich damit Malware auf den PC herunterladen. So erhielten beim ersten Angriff auf das EDA 2007 Mitarbeiter Mails mit der unverdächtigen Aufforderung, Fotos für einen Wettbewerb zu bewerten. Wer die Fotos anklickte, fing sich damit einen Trojaner ein, der ein Spionageprogramm installierte. Der Erfolg sozialer Netzwerke wie Facebook, MySpace oder Twitter bringt Hacker vermehrt auch auf diese Plattformen, um Malware zu verbreiten und an Adressen zu kommen.

Multis wie Zurich Financial Services sensibilisieren die Mitarbeitenden in Trainings für die Sicherheitsproblematik und legen mit Richtlinien fest, wie sich die Angestellten bei IT-Risiken zu verhalten haben. Geregelt ist bei der Zurich auch, welche Hardware genutzt werden darf.

Auch die Credit Suisse führt Schulungen durch und instruiert die Mitarbeiter im sicheren Umgang mit E-Mails. Matthias Friedli, Mediensprecher der Grossbank: «Unsere Weisungen und Vorschriften umfassen alle Datenträger und Kommunikationsmittel.»

Solche Richtlinien sind längst nicht überall Standard. Experten bemängeln immer wieder, dass es in vielen Firmen ►



CARAN d'ACHE
GENEVE

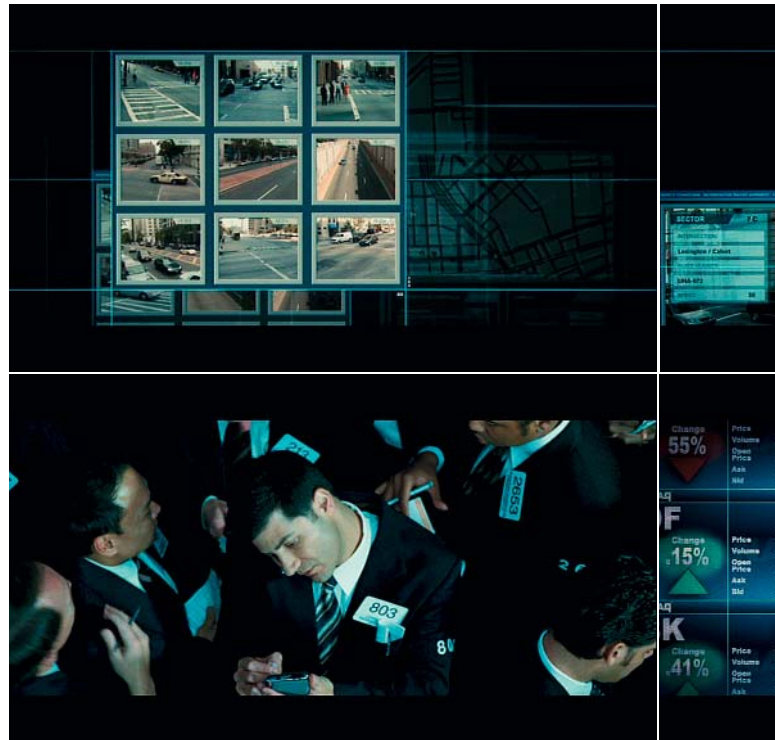
LinkSeries

Kollektion Varius
Limited Edition



Landolt-Arbenz
Bahnhofstrasse 65, 8001 Zürich, tel : 043 443 77 00
&
Gerbergasse 41/Falknerstrasse 18, 4001 Basel,
tel : 061 263 22 00
Brachard Cie.
rue de la Corraterie 10, 1211 Genève,
tel : 022 817 05 55
KramerKrieg
rue Centrale 10, 1003 Lausanne, tel : 021 345 00 95

CARANDACHE.COM



Ein gezielter Angriff auf die Wall Street hätte fatale Folgen für das globale Finanzsystem, wie «Die Hard 4» im Hollywood-Stil vormacht.

► keine klare Politik für den Umgang mit Sicherheitsrisiken gibt. Im Oktober veröffentlichte PricewaterhouseCoopers die Resultate einer Befragung von 7200 CEO und IT-Managern aus 130 Ländern. Diese ergab, dass nicht einmal eines von vier Unternehmen Richtlinien für die Nutzung sozialer Netzwerke hat. Vorgaben müssten auch regeln, ob und wie Mitarbeiter portable Speicher und Geräte wie USB-Sticks, Smartphones oder Fotokameras in der Firma nutzen dürfen, denn diese können gefährliche Fracht ins Firmennetz einschleusen. So versucht sich etwa der seit Monaten aktive Wurm Conficker über einen Trick auf USB-Sticks einzunisten.

Klare Instruktionen erfordert auch der Umgang mit E-Mails. Der weltweite Mailverkehr besteht zum überwiegenden Teil aus Spam, der in den Filtern der Provider und Mail-Server hängen bleibt. Jene Spam-Mails, die es bis ins Postfach schaffen, sind ein Risiko. Laut Websense sind über 87 Prozent aller Mails Spam, und davon locken wiederum über 80 Prozent auf Websites, die mit Malware infiziert sind. Man mag solche Zahlen mit Vorsicht geniessen, doch Websense hat Erfahrung. Die börsenkotierte amerikanische Firma bietet Sicherheitslösungen und betreibt Security Monitoring für Organisationen und Firmen mit über 44 Millionen Mitarbeitenden weltweit.

Cyber-Kriminelle setzen ihre Angriffe mitunter auch zielgruppenspezifisch ein.



Die Schweizer Melde- und Analysestelle Informationssicherung (Melani) des Bundes berichtet über eine an Firmenkader gerichtete Mailwelle, die im ersten Halbjahr dieses Jahres lief. Eine englisch abgefasste Mail mit Hinweis auf eine Zahlungsüberweisung enthielt einen Anhang, der infiziert war. Das Ziel, einen Trojaner zu verteilen, hatte auch eine andere Spam-Mail, die mit einer gefälschten Website im Look der Gratiszeitung «20 Minuten» verlinkt war und zum Anklicken eines Videos zum Bericht über osteuropäische Prostituierte einlud. Opfer von Phishing-Angriffen waren in den letzten zwölf Monaten auch Bluewin sowie die Universitäten Zürich und Basel. Hacker verschafften sich auch Zugang zu den Webservern der Stadtpolizei Zürich und des Kernforschungszentrums Cern in Genf und manipulierten Webseiten.

VON DER KRISE BEGÜNSTIGT. Alarmierend sind weitere Trends, auf die Websense im Bericht «State of Internet Security» für das erste Halbjahr 2009 hinweist. Demnach hat sich im vergangenen Jahr die Zahl der infizierten Websites versechsfacht. Besonders bedenklich: Drei von vier dieser Websites gehören seriösen Betreibern, die von der eingeschleusten Schadsoftware nichts wissen. Auch die Experten von Melani verweisen auf das gestiegene Risiko solcher Drive-by-Infektionen. Laut der Meldestelle wurden letztes Jahr zahlreiche Schwei- ▶

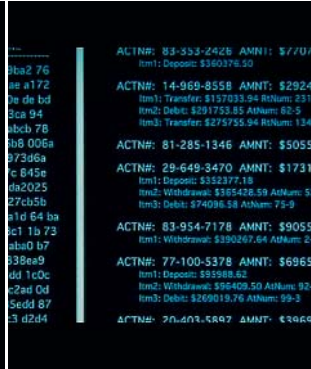
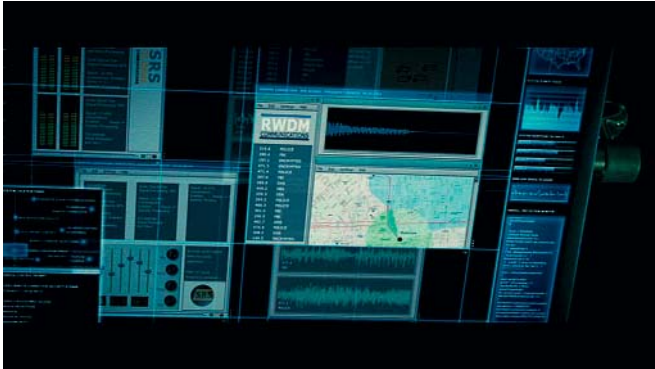
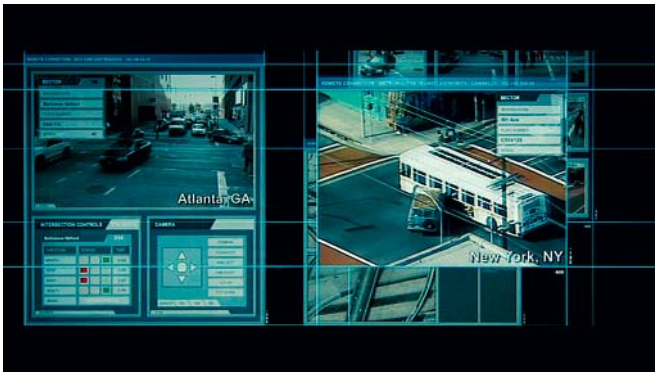
Film-Stills: Twentieth Century Fox Film Corporation

Jetzt 5000 Meilen*
 Partner of Miles & More

Unverhofft kommt oft. Immer wieder finden Sie sich in Situationen, die Sie so nicht erwartet haben. Damit Sie in Zukunft dafür gewappnet sind, sorgen wir mit unseren Socken und Unterwäsche-Abos regelmässig für frische Socken und gepflegte Wäsche. Ersparen Sie sich die Blamage und besuchen Sie uns: www.blacksocks.com

*mit jedem Unterwäsche-Starter-Kit

BLACKSOCKS™
Die Socken im Abo



► zer Websites gehackt, um bösartige Codes unterzubringen.

IT-Chefs sind zunehmend mit Herausforderungen konfrontiert, nicht zuletzt durch sicherheitsrelevante unternehmerische Entscheide. Dazu gehören etwa das Outsourcing von Diensten oder die Probleme, wenn nach Fusionen unterschiedliche Infrastrukturen und Sicherheitskonzepte zu verschmelzen sind. Gleichzeitig steigt der Kostendruck. Während die Bedrohung durch Cyberkriminalität weiter steigt, hat die Wirtschaftskrise zur Folge, dass sich viele IT-Abteilungen mit eingefrorenen Budgets abfinden müssen.

Das trifft vor allem Firmen mit Nachholbedarf. Dies sind laut der Virenspezialistin McAfee vor allem mittlere Unter-

nehmen, die dieses Jahr viel mehr Angriffen ausgesetzt waren als noch 2008. Mehr als zwei von drei befragten Chefs von Unternehmen mit 51 bis 1000 Mitarbeitern fürchten denn auch, dass eine massive Sicherheitspanne ihr Business beeinträchtigen könnte.

CYBERCRIME IM VISIER. Manche Entscheider mögen die von Sicherheitsspezialisten gemalten Szenarien als überzeichnet abtun. Tatsache ist jedoch, dass aufsehenerregende Fälle wie jener von Heartland Payment Systems oder anhaltende Phishing-Angriffe gegen Finanzinstitute ein Warnsignal sind. Lauschangriffe mit politischem Hintergrund erhöhen zudem bei Regierungen den Handlungsdruck. Umso mehr, als die Verletzlichkeit

Firewalls, geschlossene Netzwerke und Antivirenprogramme sollen für Sicherheit sorgen.

computertechnischer Infrastrukturen in der modernen Cyberkriegsführung vermehrt ausgenutzt wird. So spielten etwa 2008 im Konflikt zwischen Georgien und Russland DoS-Angriffe gegen Regierungsserver eine Rolle.

Der US-Verteidigungsminister Robert Gates hat die Schaffung einer neuen Pentagon-Einheit namens United States Cyber Command bekanntgegeben. Geplant ist auch eine neue Organisation zum Schutz der zivilen Netzinfrastruktur. Die EU rüstet sich ebenfalls im Kampf gegen die neue Bedrohungslage in der vernetzten Welt. Sie hat die Gründung einer Task Force gegen Cybercrime beschlossen. ■

Film-Stills: Twentieth Century Fox Film Corporation

ANZEIGE

WWW.REALESTATEINVESTMENT.CH

wincasa

Wincasa AG Real Estate Investment
Ihr Partner für Immobilien-Vermittlungen
Basel | Bern | Luzern | Olten
St.Gallen | Winterthur | Zürich

DIE DINGE HABEN NUR DEN WERT, DEN MAN INHNEN VERLEIHT. MÖLIERE

DEFINITIONEN

Glossar der Hacker

Eine Übersicht über die Mittelchen im Giftschrank der Cyber-Bösewichte.

► **MALWARE:** Überbegriff für Programme, die unerlaubterweise auf einem Rechner installiert oder in ein Netz eingeschleust werden, um dort Schaden anzurichten oder den Diebstahl von Informationen zu ermöglichen.

► **BOT:** Ein Programm, das einen PC per Fernsteuerung kontrollierbar macht. Ein solcher Bot-Rechner, auch Zombie genannt, wird mit Tausenden gleichermaßen infizierten Rechnern zu einem Bot-Netz zusammengeslossen, das in der Regel ohne Wissen des Besitzers für eine DoS-Attacke oder den Versand von Spam-Mails missbraucht wird.

► **DOS-ATTACKE:** Denial of Service (DoS), zu Deutsch Dienstverweigerung, ist eine Methode, um Websites lahmzulegen. Dabei bombardieren in einem Bot-Netz verknüpfte PC den Webserver permanent mit Datenpaketen, worauf dieser zusammenbricht. DoS-Angriffe können Stunden oder Tage dauern.

► **DRIVE-BY-INFEKTION:** Die Drive-by-Infektion ist besonders heimtückisch. Diese Malware kann sich allein durch den Besuch einer Website auf einen PC laden, ohne dass der Anwender etwas anklickt. Dies kann selbst auf vertrauensvollen Sites geschehen, solange die Malware unentdeckt bleibt.

► **KEY-LOGGER:** Ein auf den PC eingeschleustes Programm, das alle Tastatureingaben oder Screenshots aufzeichnet und heimlich an den Angreifer übermittelt. Damit können Passwörter und sensible Informationen ausspioniert werden.

► **PHISHING:** Mit der Betrugsmethode Phishing – ein Wortspiel aus Password und Fishing – versuchen Hacker, Zutrittsinformationen und Passwörter abzufangen. Wie der Fischer den Köder auswirft, so verschickt der Hacker Mails, in denen er sich etwa als Bankvertreter ausgibt und den Empfänger unter einem Vorwand auffordert, seine Kontodaten auf

einer gefälschten Website im Originallook einzugeben. Von Phishing häufig betroffen sind Finanzdienstleister und Auktionsplattformen.

► **SCAREWARE:** Schadprogramme namens Scareware nutzen die Angst der Anwender vor Attacken aus. Sie melden sich mit dem Hinweis, ein Virus habe das System infiziert. Gegen Bezahlung bieten sie Hilfe an, die nicht benötigt wird. Oftmals wird das Opfer zu einem Klick verleitet, der eine Infizierung überhaupt erst auslöst.

► **TROJANER:** Diese Schadsoftware wird als unverdächtige Anwendung getarnt, besitzt jedoch die Fähigkeit, andere Malware auf den PC zu laden. Der Trojaner ist nur Türöffner und führt keinen böartigen Code aus. Der Name spielt auf die Mythologie an, nach der die Griechen die Trojaner mit dem Geschenk eines riesigen Holzpfers überlisteten, in dessen Bauch sich feindliche Soldaten versteckten.

► **VIRUS:** Umgangssprachlich werden unter Viren Programme verstanden, die auf einem PC Schaden anrichten. Der Virus ist ein kleines Programm, welches das Verhalten eines Computers ändert. Er befällt ein anderes Programm und manipuliert dieses so, dass es den Virus weiterverbreitet. Viren können zerstörerisch sein, aber auch nur harmlose Aktionen auslösen.

► **WURM:** Würmer funktionieren ähnlich wie Viren, sind aber für ihre Verbreitung nicht auf einen Wirt – also ein anderes Programm – angewiesen. Sie verbreiten sich selbständig im Netzwerk, indem sie Sicherheitslücken und Konfigurationsfehler ausnützen.

► **ZERO-DAY-ATTACKE:** Eine Angriffsvariante, bei der gezielt die Zeitspanne vom Bekanntwerden von Sicherheitslücken in Programmen und Betriebssystemen bis zur Veröffentlichung des Updates genutzt wird. Das System ist dann ungeschützt.

ANZEIGE



ARVI SA
„THE SWISS BANK OF FINE AND RARE WINES“

Leading Fine Wine Merchant offers at trade prices

- Over 500'000 bottles in stock
- 5'000 different labels
- Vintages from 1811 to 2008
- Expert advice
- Investments
- World-wide delivery

ARVI SA · Via Pedemonte · 6818 Melano · Switzerland
P: +41 (91) 649 32 88 · F: +41 (91) 648 33 75 · www.arvi.ch · info@arvi.ch