

Käfer EDV Systeme GmbH

Computer - Netzwerke - Service - Grafik & Layout

Jülicher Straße 336b
D 52070 Aachen

Tel.: 0241/96877-0, Fax: 0241/96877-15, D2: 0172/2403674
<http://www.kaefer-edv.de> email: info@kaefer-edv.de



Hotline III/2005

Käfer EDV – Die tun was! Unser Sicherheitsprogramm

Nachdem wir uns in der letzten Ausgabe unserer Hotline mit dem Thema „Konjunkturbelebung in Deutschland“ auseinander gesetzt haben, wollen wir uns diesmal mit dem Schwerpunktthema Sicherheit befassen. Hierbei wollen wir es nicht bei den üblichen Ermahnungen, wie „Augen auf beim Internet-Kauf“, belassen oder nur über Viren, Würmer und Trojaner berichten, sondern darüber, wie die Medien „Internet“ und „PC“ für straf- und zivilrechtlich relevante Delikte missbraucht werden und wie Sie sich dagegen wehren können.

Konkret wollen wir aktuelle Praktiken von Betrügern und Kriminellen unter die Lupe nehmen und Sie darüber aufklären, in welche Falle Sie als gutgläubiger Konsument tappen können. Gespickt ist dies alles mit ganz persönlichen Erfahrungen aus der jüngsten Vergangenheit. Lesen Sie hier, warum mich die Firma Weightwatchers® abmahnte und wie es uns mit Hilfe der Aachener Kriminalpolizei gelang, den Diebstahl unseres Firmenwagens mittels einem fingierten Ankaufangebot als Antwort auf unser Internetinserat bei mobile.de zu vereiteln.

Bedrohungsszenarien

Meine diesjährige Sommerreise durch Frankreich und Italien führte mich u.a. auch in die Festungsstadt Carcassone im Südwesten von Frankreich an den Ausläufern der Pyrenäen. Die Festung gilt als die größte weitestgehend vollständig erhaltene Burganlage in ganz Europa und erhebt sich in Ihrer Größe beeindruckend über das Umland und die jüngeren Stadtteile von Carcassone. Dadurch, dass sie bereits im 19. Jahrhundert restauriert wurde, wirken auch die wieder aufgebauten Bestandteile der Festungsanlage authentisch. Diese einmalige Kulisse wurde unter anderem für Filmaufnahmen zu Robin Hood mit Kevin Costner genutzt.

Versetzt man sich nun in die Lage der Menschen, die damals solche Festungen erbaut haben, so erkennt man, dass diese einem einzigen Zweck dienten: Schutz vor einer Bedrohung durch fremde Eindringlinge und Eroberer. Dass die Gemäuer auf unsere heutige Zivilisation eine romantische Anziehungskraft haben und Jahrhunderte später als Touristenattraktion Hunderttausende Besucher jährlich anlocken würden, hatte bei der Planung der Festungsanlage wohl niemand im Kalkül.

Die Festung in Carcassone besteht aus drei Ringen: einer vorgelagerten Mauer mit Wehrgängen und einem einzigen Tor, einer äußeren Stadtmauer mit Wachtürmen und im Zentrum einer inneren Mauer mit Wassergraben und weiteren Wehrtürmen.

Die gesamte Anlage ist zudem auf einem Hügel gebaut und bietet einem Angreifer allein dadurch schon geografische und physikalische Nachteile. Eigene Brunnen und entsprechend große Vorratskammern machten die Anlage für ihre Bewohner im Ernstfall zu einer praktisch uneinnehmbaren Trutzburg. Hatte ein Angreifer es tatsächlich geschafft, mit Hilfsmitteln, wie Leitern und Podesten die erste Mauer zu überwinden, stand er nun eingeklemt zwischen erstem und zweiten Ring ohne weitere Hilfsmittel da und vor der Aufgabe, die weit höhere Mauer ohne technisches Gerät zu überwinden. Möglicherweise sah er sich nun selber Angriffen der Verteidiger ausgesetzt. Selbst wenn der nächste Wall auch fiel, der Weg durch die engen Gassen zum inneren Ring mit Wassergraben wurde jetzt noch gefährlicher und beschwerlicher.

Die größte Gefahr für die Bewohner bestand dann wohl auch ausgehend von ihr selber. Es reichte nur eine Unachtsamkeit am Tor oder vielleicht bei der Nutzung eines Geheimganges aus der Festung heraus, ein Verbündeter in der Festung (Trojaner) oder schlichtweg die Ungeduld der eingeschlossenen, um den Belagern doch einen Weg in die Stadt zu gewähren.

Was hat das mit IT-Sicherheit und Internet zu tun? Eine ganze Menge, wie ich finde. Wir leben zumindest in unseren Breitengraden Gott sei dank nicht mehr in Gebieten und in einer Zeit, in der wir den hinterhältigen Angriff der Barbaren mit Schwert und Axt fürchten müssen. Unsere Schlachtfelder sind subtiler geworden, deutlich weniger grausam, in ihrer wirtschaftlichen oder persönlichen Konsequenz jedoch nicht minder gefährlich.

Der heimische PC ist längst keine Schatztruhe privater Geheimnisse mehr, der Firmen-PC weder sicher vor den eigenen Kollegen oder dem Chef noch vor der Konkurrenzfirma oder zwielichtigen Gestalten, die Daten anstelle von Handtaschen rauben. Das Internet mit all seinen Vorzügen der modernen, schnellen und effizienten Kommunikation und Recherchemöglichkeiten hat die Inseln der Sicherheit durch unsichere Strassen und Wege miteinander verknüpft. Jeder Computer, der heute in irgendeiner Form mit der Außenwelt verbunden ist (und sei es allein nur durch die Möglichkeit des physikalischen Zugangs zu Tastatur und Bild-

schirm) ist heute ein potentielles Ziel für die Barbaren des 21. Jahrhunderts.

Eine Firewall als Analogie zu dem Befestigungswall der Burg, die den einzelnen PC oder das ganze Netzwerk von Angriffen von außen schützt, funktioniert nur dann, wenn der Durchfluss der Daten absolut unter Kontrolle ist. Schläft die Wache am Stadttor, so nistet sich Gesindel in Form von Datendieben und Spitzeln ein und öffnet von innen das Tor, wenn alles schläft.

Um mich und meine EDV also wirklich schützen zu können, muss ich wissen, welches Bedrohungspotential auf welchen Wegen auf mich lauert.

Angriffe von außen

Die Bedrohungs-Szenarien, die von außen an ein EDV-System herangetragen werden, sind sicherlich vielfältiger und weit verbreiteter, als die, die Ihren Ursprung im Inneren des Netzwerkes bzw. des Unternehmens haben. Gilt ein IT-System ohne Kommunikationsschnittstellen nach außen (Online, Datenträgeraustausch etc.) per se als sicherer (wenn man den lokalen Zutritt zum System aus der Betrachtung herausnimmt), so ändert sich das Bedrohungspotential bei einer Online-Anbindung nach außen deutlich.

Würmer und Trojaner

In der Praxis gibt es dabei i.d.R. weniger direkte und gezielte Hack-Angriffe von außen auf ein EDV-System, sondern vielfach eine über Würmer und Trojaner ausgelöste meist unkontrollierte Versendung von vertraulichen Daten von innen nach außen. Sicherlich stehen bestimmte Firmen und Institutionen ganz oben auf der Wunschliste von Hackern und Spionen (z.B. Firmen wie Microsoft®, Rüstungsunternehmen oder Einrichtungen der öffentlichen Hand), in der Vielzahl der Fälle sammeln Hacker jedoch Informationen in der Breite der Masse über Trojaner¹, um sie dann gezielt nach verwertbarem Material zu durchforsten.

¹ Trojaner: Malware / Programme, die sich in einen PC unbemerkt einnisten und im Hintergrund Daten versenden oder Hintertüren für weitere Hacker-Attacken öffnen

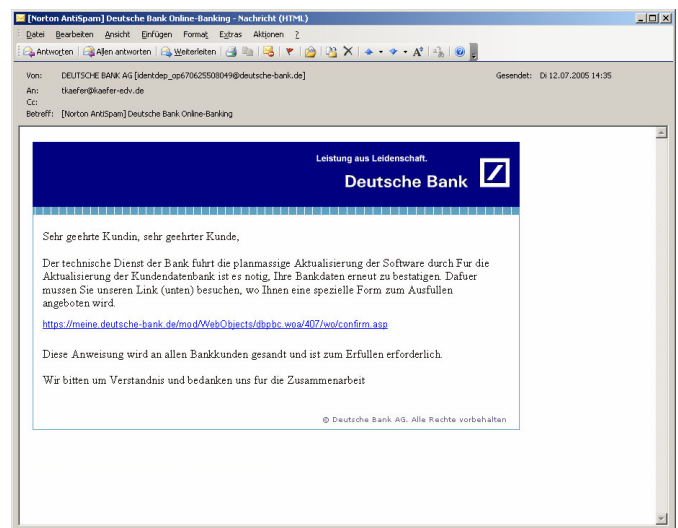
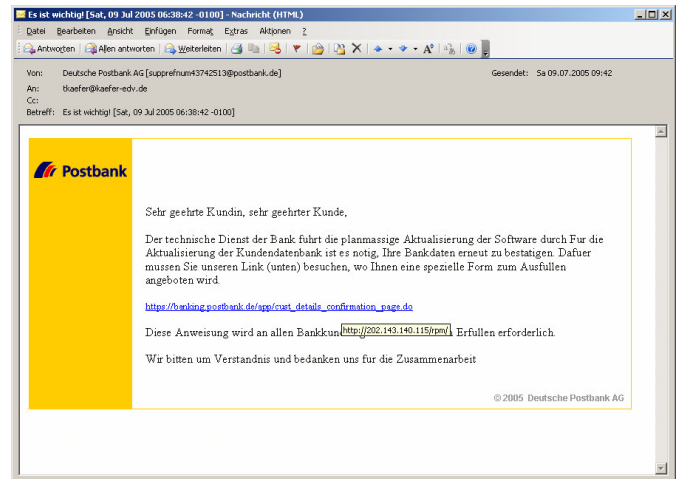
Direkte Angriffe

So ist der einzelne Rechner oder ein Firmennetzwerk oft aus dem Internet gar nicht ohne Kenntnis bestimmter, ständig wechselnder Informationen zu identifizieren, so dass eine gezielte Attacke hier nur mit erhöhtem Aufwand und Insider-Kenntnissen realisierbar ist. Bei der Einwahl ins Internet erhält man von den meisten Provider i.d.R ständig wechselnde TCP/IP-Adressen über die das Netzwerk dann erreichbar ist. Ohne Kenntnis der aktuellen IP-Adresse ist somit der gezielte Angriff auf ein Netz nicht möglich. Daher versucht man durch entsprechend versuchte Emails oder Webseiten so genannte Würmer und Trojaner in die Systeme einzuschleusen, die dann, einmal im Wirts-System eingeknistet, von sich aus für die Verbreitung von sensitiven Daten an vorher festgelegte Ziele sorgen. So versucht man beispielsweise mit einem Key-Logging sämtliche Tastenanschläge des Benutzers mitzulesen, um auf diese Art und Weise z.B. Passwörter für andere Systeme, wie z.B. Online Banking, mitzuschreiben.

Phishing

Eine andere, mittlerweile sehr verbreitete Form der Datenausspähung ist das so genannte „Phishing“. Dieses Kunstwort beschreibt das „Passwort Fishing“, d.h. das Fischen nach Passwörtern beispielsweise im Email- und Online-Verkehr durch Umleiten von Benutzereingaben auf entsprechend präparierte Web-Seiten. Hierbei wird z.B. eine offiziell aussehende Email mit Logo und Layout der entsprechenden Unternehmen, wie z.B. Microsoft®, Ebay® oder Bankinstituten, per SPAM-Verfahren massenhaft an verschiedenste Empfänger verschickt und diese darin aufgefordert, sich bei dem entsprechenden Dienst anzumelden, um z.B. die Vertragsdaten zu aktualisieren. Wer z.B. öfters über Ebay® einkauft wird sich möglicherweise nichts dabei denken, wenn er eine „gut“ gemachte Nachricht erhält, in der er aufgefordert wird, sein Passwort aus Sicherheitsgründen zu ändern. Der nachfolgende Einlog-Vorgang, der dann über die in der Email enthaltenen Hyperlinks erfolgt, verbindet Sie dann jedoch nicht mit dem richtigen Online-System Ebay®, sondern wird von einem Hacker-System abgefangen.

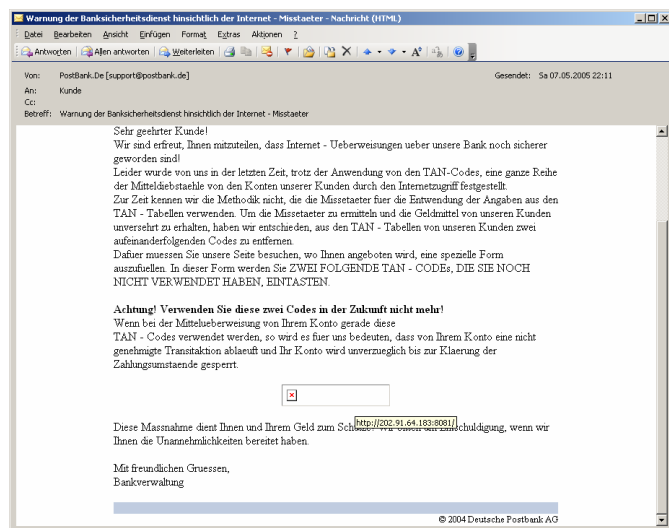
Zu identifizieren sind solche Tricks meist an optischen Auffälligkeiten, wie manchmal recht schwache Orthografie oder umständlicher Formulierungen. Zudem unterscheiden sich die Hyperlinks, die sich hinter den anklickenden, offiziell wirkenden Texten verbergen, von den angezeigten Zieladressen.



In der Regel wird kein Unternehmen auf seine Kunden per E-Mail zugehen und dazu auffordern, geheime Zugangsdaten oder Legitimationsnachweise erneut einzugeben. So ist auch nachfolgend gezeigte Aufforderung, zur Eingabe von zwei aufeinander folgenden TAN²-Nummern zur Absicherung der gesamten Liste nur ein Trick, um an unverbrauchte TANs samt PIN und Kontonummer zu gelangen. Der Betrüger überweist dann mit den so gewonnenen TANs Geldbeträge von Ihrem

² TAN: Transaktionsnummer – einmalig gültige Nummer zur Legitimation z.B. einer einzigen Überweisung beim Online-Banking; wird als Liste vom Kreditinstitut ausgegeben.

Konto auf sein eigenes und verschwindet kurze Zeit später „auf Nimmerwiedersehen“. Diese E-Mails werden massenhaft über die gleichen Wege wie Werbemüll (SPAM) wahllos an hunderttausende von Adressen verschickt. Sie können sicher sein, dass es genügend Leute gibt, die dann tatsächlich ein Konto z.B. bei der Postbank oder der Deutschen Bank haben und der Aufforderung ohne Argwohn folgen. Bis die Adressen, auf die die Umleitungen verweisen, dann im Internet blockiert werden (Errichtung von Straßensperrungen, um beim Eingangs-Beispiel zu bleiben), vergehen meist Tage. Genügend Zeit, um selbst bei einer Rücklaufquote von wenigen Promille einen „ordentlichen“ Schaden anzurichten.



Wohlgermerkt ist dies nicht ein Problem speziell der Postbank oder der Deutschen Bank. Hier wird viel mehr der Umstand genutzt, dass diese überregional tätigen Kreditinstitute die potentiell größte Chance für die Betrüger bieten, mit Ihrer Email tatsächlich auch einen Kunden dieses Instituts zu erreichen.

Man-in-the-middle-Attacken

Die „Perfektion“ solcher Angriffe sind dann die „Man-in-the-middle-Attacken“, bei denen sich der Angreifer in die Kommunikation zwischen Anwender und Anbieter schaltet und die Eingaben und Ausgaben der Systeme manipuliert. Gelangt solch ein Angreifer beispielsweise in die Kommunikation mit dem Bank-Institut beim Online-Zahlungsverkehr, so ist es dem Angreifer möglich, die Eingaben des Benutzers mitzuschreiben und z.B. für Kontostandabfragen an die Bank weiterzuleiten und das Ergebnis dem Nutzer auch 1:1 wei-

terzureichen, um ihn in Sicherheit zu wiegen. Bei einer nachfolgenden Transaktion (Online-Überweisung) jedoch leitet er die Eingaben nicht an die Bank weiter, sondern simuliert die Antworten der Bank lediglich. Nachfolgend überweist er dann mit Hilfe der mitgeschriebenen Passwörter und TAN-Nummern einen Geldbetrag auf ein von ihm kontrolliertes Konto. Der Nachweis einer solchen Manipulation ist dann nicht einfach und der Anwender wird möglicherweise beweispflichtig. Auch das neuerdings von den Geldinstituten als „sicher“ propagierte ITAN-Verfahren gilt unter Fachleuten auch als unsicher!

Sichere Kommunikation

Um dies zu vermeiden, bedient man sich daher sinnvollerweise gerade bei kritischen Übertragungen entsprechende gesicherter Verfahren wie beispielsweise der SSL-Kommunikation oder Online-Banking-Standards wie z.B. dem HBCI Verfahren³. Manipulationen sind zwar auch hier nicht ausgeschlossen, jedoch deutlich schwieriger zu bewerkstelligen als bei ungesicherten Verfahren. So bringen solche Verfahren in Kombination mit speziellen Online-Banking-Programmen, wie z.B. Star-money®, Sfirm® usw. Sicherheitsvorteile, da hier eine von den Programmen gesteuerte und überwachte Übertragung stattfindet und keine unsichere Kommunikation über Web-Browser durch den Benutzer initiiert wird.

Fernwartung

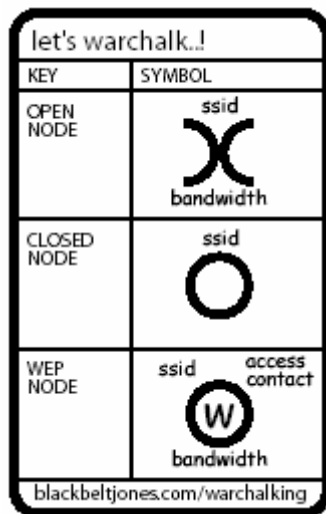
Besonderen Augenmerk gilt es Fernwartungszugängen zu schenken. Mittels Fernwartungszugängen werden für externe Benutzer oder IT-Dienstleister Zugänge zum EDV-System geschaffen, mit denen diese i.d.R. einen Vollzugriff auf das interne System erhalten. Mit Programmen wie z.B. VNC, PC-Anywhere® oder dem in neueren Windows®-Versionen enthaltenen Remote-Desktop ist es möglich, ein anderes System so zu steuern, als würde man direkt davor sitzen. Was im Problem- und Fehlerfall ein Segen sein kann und schnelle Hilfe ermöglicht, kann im Missbrauchfall katastrophal sein. Ein gehackter Fernzugang kann so z.B.

³ HBCI: Homebanking Computer Interface: auf Chipkarten oder Diskettenlegitimation aufbauende, multibankfähige Schnittstelle zur verschlüsselten und gesicherten Kommunikation mit Kreditinstituten

in der Nacht bei laufendem Netzwerkserver als ausgiebig nutzbare „Spielwiese“ für einen Hacker dienen. Aus diesem Grund sollte der Fernzugang entsprechend gesichert sein, Passwörter öfters gewechselt werden und der Personenkreis für den Zugriff auf das absolut notwendige und vertretbare Maß reduziert sein. U.U. sind hier auch rechtliche oder standesrechtliche Vorgaben zu berücksichtigen, wie beispielsweise die Empfehlung der Bundesärztekammer, Fernzugriff auf Patientendaten grundsätzlich zu verbieten oder nur mit Aufsicht durch den Arzt zuzulassen.

Wireless LAN

Eine Schwachstelle beim Ausspähen von Daten sind die in den letzten Jahren in Mode gekommene WLAN's, Funknetze also, die häufig auch in kleinen Büros, Praxen oder Heimnetzen zu finden sind. Da die Funknetze Bestandteile des eigentlichen Netzwerkes sind und somit eine Verbindung zu den zu schützenden Daten besitzen, andererseits aber aufgrund der physikalischen Eigenschaften der Funkwellen weit über die Räumlichkeiten hinaus abhörbar sind, gilt es gerade hier, besonderes Augenmerk auf Verschlüsselung und Absicherung zu werfen. Man schätzt, dass noch rund die Hälfte der WLAN's in Deutschland vollkommen offen betrieben werden, begründet durch die standardmäßige Deaktivierung aller Sicherheitsmaßnahmen und die Unwissenheit der Betreiber, die die Geräte oft in Eigenregie „out of the box“ installieren und sich über die „gelungene“ Standardinstallation freuen. So genannte „War Chalkings“ an den Hauswänden zeigen dann von „War Drivern“⁴ gefundene, offene Netzwerke an. Sollten Sie also an Ihrer Hauswand Zeichen wie diese finden, sollten Sie Ihr Funk-LAN von einem Fachmann absichern lassen.



Ein sehr „amüsantes“ Erlebnis hatte ich bei einem Besuch eines Freundes vor wenigen Tagen. Wir hatten uns bei ihm zuhause getroffen, um ein paar Dinge zu besprechen. Um ihm etwas näher zu erklären, packte ich mein Notebook aus und wollte ihm eine Datei zur Erläuterung zeigen. Beim Hochfahren meldete mein Notebook „Ungesichertes Funknetzwerk gefunden!“ und warnte mich, mich mit diesem zu verbinden, da dann eine abhörbare Verbindung zwischen dem Funknetzwerk und meinem Laptop aufgebaut würde. Mehr noch – Hätte ich auf meinem PC ungesicherte Netzwerkfreigaben gehabt (und die hat man in der Regel im Auslieferungszustand von Windows-Systemen), so hätte ein Fremder in Funkreichweite sofort auch auf mein Notebook zugreifen können. Ich ahnte natürlich sofort, was Sache war und bedankte mich schmunzelnd bei meinem Freund für den kostenfrei zur Verfügung gestellten Internetzugang, denn 10 Sekunden später war ich ohne weiteres Zutun mit der Startseite von Google verbunden und surfte nun demonstrativ im Internet.

Das Erstaunen meines Freundes war natürlich groß, hatte er doch geglaubt, bei der Installation seines Routers alles richtig gemacht zu haben. Sein Erstaunen wich leichtem Entsetzen, als ich nach weiteren 15 Sekunden die Anmeldemaske seines Funk-Routers auf meinem Schirm hatte (eine Kleinigkeit für einen IT Fachmann). Praktischerweise stand direkt neben dem Passwortfeld zum Login „0000 bei Auslieferungszustand“. Das lies ich mir natürlich nicht zweimal vorschlagen und versuchte das vorgeschlagene Passwort. Wenigstens das hatte er geändert und ich kam an dieser Stelle erst einmal nicht so ohne weiteres weiter. Hätte er das Passwort nicht geändert, hätte ich ihm seine Konfiguration problemlos sperren können, so dass er selber nicht mehr an das System gekommen wäre. Ein Blick in die Konfiguration zeigte dann auch schnell die gemachten Fehler: Der WEP-Modus war statt eingeschaltet. Auch wenn die WEP-Verschlüsselung nachweislich nur wenig absolute Sicherheit bietet, sollte man sie oder besser die zuverlässigere Alternativen WPA oder 802.11x nutzen, um Schmalspur-Hackern wie mir, das Leben nicht ganz so einfach zu machen. Hätte er dann auch noch die SSID versteckt und die zugelassenen Endgeräte mittels MAC-Authentifizierung eingetragen, hätte einer weitestgehend sorgenfreien Nutzung des Funknetzes nichts im Wege gestan-

⁴ War Driver suchen mit Auto und Notebook durch Umherfahren in Städten nach offenen Funknetzen und katalogisieren diese in entsprechenden Karten

den. Tja, wenn er denn überhaupt eins gebraucht hätte: An den Router war lediglich ein PC per Kabel angeschlossen. Die Funkfunktionalität war im Router quasi kostenlos enthalten gewesen und er hatte sie wider besserer Empfehlung eingeschaltet und das Stadttor weit offen gelassen (um jetzt wieder das Beispiel Carcassone aufzugreifen). Seine Nachbarn werden jetzt wahrscheinlich enttäuscht sein, dass sie nicht mehr kostenlos im Internet surfen können und die Bikini-Fotos seiner Frau von seinem PC herunterladen können ☺. Aber das ist nur eine Vermutung meinerseits, denn als ich dort wegfuhr, sah ich keinen seiner Nachbarn mit dem Notebook umherwandern, um nach neuen Empfangsmöglichkeiten zu suchen.

Angriffe von Innen - Social Engineering

Die Bedrohungs-Szenarien Datenausspähung, -manipulation und -zerstörung entspringen aber nicht immer dem „bösen“ Internet oder der Außenwelt, sondern haben ihre Quelle oder die undichte Stelle oft auch im eigenen Netz (Social Engineering). Ein unzufriedener oder vor der Entlassung stehender Mitarbeiter hat schon oft Daten zerstört oder zur späteren (missbräuchlichen) Nutzung entwendet. Da kein System der Welt als 100% sicher vor Einbrüchen und Manipulationen angesehen werden kann und faktisch jede noch so ausgeklügelte Sicherheitsbarriere mit entsprechendem Aufwand umgangen werden kann, kommt der Feststellung, **dass** es einen konkreten Angriff auf die EDV gibt oder gab und nachfolgend der entsprechenden Beweissicherung, immer mehr Bedeutung zu. Gerade für Unternehmen, die für Angreifer ein lukratives Ziel darstellen bzw. deren EDV für das tägliche Geschäft als Herzstück oder Rückrat zu bezeichnen ist, ist es äußerst empfehlenswert, sich frühzeitig **vor** einer Bedrohung Gedanken über Alarmierungssysteme (Intrusion Detection) und konkrete Ablaufpläne im Schadensfall zu machen (Incident Response).

Bei einem tatsächlichen Vorfall kollidieren fast immer zwei gegensätzliche Interessen. Auf der einen Seite wird man bemüht sein, ein z.B. mit einem Virus oder Trojaner befallenes System schnellstens wieder im Produktiveinsatz nutzen zu können. Andererseits ist bei einem entstandenen Schaden oder dem Verdacht auf systematische und strafbare Handlungen die konzeptionell richtig

angelegte Beweissicherung elementar wichtig, jedoch auch sehr aufwändig. Ein kleiner Fehler, wie allein das bloße Herunterfahren des kompromittierten Systems, machen es dem Analytiker u.U. schon unmöglich, wichtige Beweise zu sichten und zu sichern, die in einem möglichen späteren Gerichtsverfahren entscheidend für dessen Ausgang sein werden.

Incident Response

Es gibt also ein paar Grundregeln, die beachtet werden müssen, wenn der Fall der Fälle eintritt und der Verdacht oder konkrete Hinweise bestehen, dass ein Computer oder ein Netzwerk von Fremden angegriffen („gehackt“) wird oder wurde bzw. wenn aus anderen Gründen eine analytisch wie rechtlich sichere Untersuchung an der EDV-Anlage vorgenommen werden soll. Im Idealfall erstellt ein Unternehmen **vor** einem konkreten Fall einen allgemeinen Notfall- und Alarmierungsplan, der den zuständigen Mitarbeitern zugänglich gemacht wird. Man bezeichnet die (strukturierte) Reaktion bei einem Verdachtsfall als „Incident Response“. Elementar für die nachfolgende Beweissicherung und Analyse der Erkenntnisse ist, dass an dem betroffenen System keine Veränderungen vorgenommen werden und der Zugang zu diesem auf das absolute Minimum an Personen begrenzt wird (Authentizität des Beweises). Sämtliche Schritte, die ab der Alarmierung durchgeführt werden, sind lückenlos zu dokumentieren. Frühzeitig wird hierbei auch eine Unterscheidung stattfinden, ob es sich tatsächlich um eine missbräuchliche Nutzung eines EDV-Systems oder nur um eine „normale“ Betriebsstörung handelt.

Der Tod vieler Beweise sind in der frühen Phase übereifrige Anwender und Administratoren, die z.B. auf erkannte Fehlfunktionen (Dialer-, Viren oder Trojaner-Befall) oder Hackerangriffe durch Herunterfahren des Systems oder gar durch Löschen von verdächtigen Programmen und Registrierungsinformationen reagieren. Hierdurch werden fast immer wichtige Beweise zerstört bzw. die nachfolgende Analyse, was genau auf dem Computer-System manipuliert wurde, erschwert. Der aktuelle Speicherinhalt des Rechners ermöglicht u.U. sehr aufschlussreiche Analysen bzgl. der aktiven Prozesse und Spuren, die bei der letzten Aktion hinterlassen wurden. Durch das Herunter-

fahren eines Systems jedoch werden die Inhalte des flüchtigen Speichers (RAM) und temporär angelegte Dateien gelöscht und der Inhalt und Status unzähliger Systemdateien verändert. Das erneute Hochfahren eines Rechners wiederum verstärkt diese Manipulationen nochmals erheblich. Bei einem Windows[®]- oder Linux-System mit entsprechendem Desktop werden in der Startphase rund 1000 Dateien „angefasst“ und so u.a. die Dateiattribute „Letzter Zugriff“ oder „Letzte Änderung“ verstellt. Ein Grundsatz des Incident Response lautet daher: „Eingeschaltete Geräte bleiben eingeschaltet und ausgeschaltete Geräte bleiben ausgeschaltet!“. Um eine möglicherweise noch bestehende und missbräuchlich genutzte Kommunikationsverbindung in das lokale Netzwerk oder zu externen Zielen (Internet, DFÜ- und Remote-Access-Zugänge usw.) zu unterbinden, sollte maximal die Kommunikationsleitung zum Endgerät selbst getrennt werden (LAN- oder Telefon-Kabel). Sofern eine konkrete Attacke zu diesem Zeitpunkt noch andauert, ist die Dokumentation des Verbindungsstatus z.B. bei einer Wählverbindung vor dem Trennen der Verbindung natürlich sehr wichtig. Oft sind auf dem System entsprechende Monitorprogramme aktiv, die auf einfachste Weise z.B. die Nutzung der ISDN-Kanäle durch eine ISDN-Karte anzeigen (Beispiel ISDN-Watch der AVM Fritz![®]-Karte). Die hier gezeigte Rufnummer sollte am besten durch Zeugen und durch Abfotografieren des Bildschirms mit einer Digital-Kamera dokumentiert werden. Das Erzeugen eines Bildschirm-Screenshots mit den üblichen Mitteln sollte unterbleiben, da hierdurch bereits wieder auf dem zu untersuchenden System Daten erzeugt werden, die die spätere Analyse möglicherweise beeinträchtigen. Überhaupt muss gerade in der ersten Phase des Incident Response darauf geachtet werden, dass die Änderungen an den Systemen so minimal wie irgend möglich ausfallen bzw. ganz unterbleiben. Dazu gehört auch das äußere Umfeld eines Computers.

Hinzuziehung von Fachleuten

Verdichten sich die Hinweise, dass eine missbräuchliche Benutzung des Computers vorliegt, so sind je nach Sachlage schnellstens die entsprechend zuständigen Fachleute zur Beweissicherung zu verständigen. Sofern der Verdacht auf eine strafrechtlich relevante Konsequenz des Vorfalles vor-

liegt, so sind unbedingt in einem ersten Schritt die Ermittlungsbehörden einzuschalten. Die Polizei-Präsidien unterhalten zu diesem Zweck entsprechend mit Fachleuten ausgestattete Kommissariate, die die Ermittlung aufnehmen. Grundsätzlich nimmt jede Polizeidienststelle eine entsprechende Anzeige auf und leitet sie weiter, jedoch ist es auch hier sinnvoll, im Vorfeld ohne eine konkrete Bedrohung bereits mit den lokalen Behörden Kontakt aufzunehmen und die Zuständigkeiten zu erfragen. Diese Kontaktdaten ermöglichen dann im Rahmen des Alarmierungsplanes deutlich schnellere Reaktionszeiten der Ermittler.

Liegt nach Auffassung der mit dem Incident Response beauftragten Mitarbeiter zunächst kein offenkundig strafrechtlich relevanter Hintergrund vor, so kann und sollte die private Beauftragung eines mit der Forensik betrauten Fachmannes (meist in Form eines EDV-Sachverständigen oder einer auf die Analyse spezialisierten Fachfirma) umgehend erfolgen. Bis zu dessen Eintreffen bleibt die Anlage unter Verschluss. Nicht wenige Gerichtsverfahren sind in der Folge daran gescheitert, dass obwohl es in der Sache selbst stichhaltige Erkenntnisse gegeben hat, die aus Sicht des Technikers für eine Beweisführung vollkommen ausreichend gewesen wären, diese in einem Verfahren nicht gewertet wurden, weil zu viele Personen Zugang zu den Beweisstücken und damit ebenfalls eine Manipulationsmöglichkeit hatten.

Zusammengefasst gehören in einen Alarmierungsplan also u.a. folgende Punkte:

- Nennung der bei Alarmierung zuständigen und für die Einleitung weiterer Schritte befugten Personen im Unternehmen
- Grundsätzliche Verhaltensregeln für die beteiligten Personen (Anwender etc.)
- Lückenlose Dokumentation der Geschehnisse und Umstände
- Eingrenzung des Zugangs zum kompromittierten System
- Keine oder nur absolut notwendige unmittelbare Eingriffe in das System
- Umgehende Hinzuziehung von (anerkannten) Fachleuten zur Beweissicherung

Datenschutz und Persönlichkeitsrechte

Von betriebsinternen Analysen und Beweissicherungsverfahren kann im Hinblick auf die Objektivität und Unabhängigkeit des Analytikers (Befangenheit) und natürlich auch aufgrund der meist nicht oder nicht ausreichend vorhandenen fachlichen Kompetenz nur dringend abgeraten werden.

Hinsichtlich des Datenschutzes und der Berührung von Persönlichkeitsrechten gilt es bei der forensischen Analyse u.a. auch, die hierbei gewonnenen Erkenntnisse absolut vertraulich zu verwenden und die Daten nach Abschluss des Verfahrens zuverlässig zu zerstören. Bei einer fachmännischen Analyse sind Informationen auffindbar, die vom Nutzer (Opfer) verloren oder zuverlässig gelöscht geglaubt sind. Allein aus diesem Grund empfiehlt sich die Hinzuziehung eines Sachverständigen, ist er doch aufgrund seines Standes u.a. zur Verschwiegenheit verpflichtet. Nur nebenbei bemerkt sei an dieser Stelle, dass natürlich alle folgend gezeigten forensischen Methoden auch firmen-intern eingesetzt werden könnten, um z.B. Informationen über Mitarbeiter und deren gespeicherte Daten zu erlangen. Dieses Ausspähen mit privater Beauftragung hat jedoch sehr schnell arbeits- oder gar strafrechtliche Konsequenzen, die vor einer entsprechenden Aktion rechtssicher geklärt werden müssen.

Identitätsdiebstahl

Wie schnell die missbräuchliche Verwendung von personenbezogenen rechtliche Konsequenzen für den Geschädigten nach sich ziehen kann, zeigt der Fall, der mir persönlich von wenigen Wochen passiert ist.

Eines Abends erhielt ich einen Anruf von einer mir unbekannt Person auf meinem Privatanschluss, die mir mitteilte, dass mein Ebay-Account gesperrt worden wäre und dass wir uns von Ebay her kennen würden. Sie hätte bei mir Produkte von Weightwatchers® (auf das ® muss ich besonders achten, damit ich nicht wirklich Ärger bekomme) ersteigert. Man kann mir ja viel nachsagen, auch dass ich mehr auf meine Ernährung achten müsste, aber tatsächlich habe ich das System bisher noch nicht angewendet, geschweige denn, irgendwelche Produkte, die damit auch nur im entferntesten zu tun hätten, versteigert oder angeboten. Ich fragte dann weitere Details ab und erfuhr, dass offenbar

jemand anderes mit meinem Namen und mit meiner Adresse Geschäfte über Ebay machte. Einzig die Emailadresse stimmte offenbar nicht. Das manifestierte sich zwei Tage später, als ich an meine Privatadresse eine Unterlassungsaufforderung einer großen, international tätigen Rechtsanwaltskanzlei erhielt, die die Firma Weightwatchers® bzgl. Markenrechtsverletzungen vertritt. Nach kurzen eigenen Recherchen in Ebay, stellte ich fest, dass es tatsächlich den genannten Benutzer-Account gab, über den in den vergangenen drei Wochen offenbar rund 100 Transaktionen von Produkten mit Rechten in Besitz von Weightwatchers® getätigt worden waren. Eine Klärung mit Ebay ergab, dass der Benutzername tatsächlich bereits gesperrt worden war und für mich glücklicherweise, dass mein echter Ebay-Account davon unberührt blieb. Nachfolgend habe ich Anzeige gegen unbekannt bei der Staatsanwaltschaft Aachen eingereicht und die Rechtsanwaltskanzlei über den offensichtlichen Identitätsdiebstahl unterrichtet. Für mich ist die Sache damit praktisch ohne nennenswerten Schaden verlaufen und es besteht die Hoffnung, dass der Täter über die bei Ebay hinterlegten Bankdaten letztlich ausfindig gemacht werden kann. Aber es hätte auch schlimmer kommen können. Allein das Sperren meines legitimen Ebay-Accounts hätte mir die Teilnahme an der Auktionsplattform incl. des darin erworbenen guten Namens auf Jahre unmöglich machen können.

An Personen bezogene Daten heranzukommen, die auch einer Schufa-Auskunft standhalten, ist sehr einfach. Sie brauchen neben Name und passender Adresse nur noch die Bankverbindung und vielleicht noch das Geburtsdatum der Person. Diese Daten in meinem Fall über das Internet herauszubekommen ist sehr einfach, bin ich doch mit Firma und als freiberuflicher Sachverständiger mit diesen Daten auf unseren Webseiten und Geschäftsdokumenten genügend oft vertreten. Forschen Sie doch mal nach sich selber: www.google.de und dann den eigenen Namen und vielleicht noch die Stadt eingeben. Sie werden ihr blaues Wunder erleben.

Fahrzeugverkäufe über das Internet

Da wir schon einmal bei den persönlichen Erlebnissen sind, will ich Ihnen die aktuellste und sicher-

lich spektakulärste Aktion in dieser Reihe nicht vorenthalten.

Als wieder einmal der turnusmäßige Austausch meines Firmenwagens anstand, bediente ich mich auch da wieder dem Medium Internet, um das alte Fahrzeug kostengünstig und effektiv zum Verkauf anzubieten. U.a. inserierte ich dazu mehrmals in diversen Autobörsen wie autoscout24.de, webauto.de und mobile.de. Nachdem sich der Angebotspreis offenbar für ausländische Autohändler auf einem interessanten Niveau eingependelt hatte, erhielt ich an einem Nachmittag gleich zwei telefonische Anfragen kurz hintereinander. Beiden Anrufern versprach ich einen Rückruf, der auch zwecks Preisverhandlung erfolgte (Wichtig: Merke 1. ohne Rückrufnummer kein Geschäft). Mit einem offenbar holländischen Händler, nennen wir ihn hier einmal Herr van den Haag, wurde ich einig und wir vereinbarten einen Besichtigungstermin am Büro für den nächsten Morgen 8.00 Uhr. Herr van den Haag wollte hierzu einen Mitarbeiter schicken, denn er selber müsste schon um 9.00 Uhr im Büro sein. Der Mitarbeiter würde Unterlagen und Vollmachten mitbringen, damit ich die über Tag in Ruhe prüfen könnte, denn das Fahrzeug sollte nach Holland ausgeführt und daher über eine Umsatzsteuer freie Rechnung nach EU-Recht deklariert werden. Dazu muss der Rechnungsaussteller die vom Rechnungsempfänger mitgeteilte Umsatzsteuer-Identnummer beim Bundesamt für Finanzen mit Sitz in Saarlouis überprüfen, da er ansonsten u.U. für die Entrichtung der Umsatzsteuer herangezogen wird.

Am nächsten Morgen stand dann auch tatsächlich ein junger Mann vor der Tür, der die versprochenen Papiere mitbrachte (Merke: 2. Namen merken und Ausweis zeigen lassen, Autokennzeichen notieren – Schade, habe ich nicht gemacht...). Der Mitarbeiter des Autohändlers schaute sich den Wagen exakt 45 sec. an, öffnete lediglich die Fahrertür und meinte nach einem kurzen prüfenden Blick ins Innere des Wagens: „Der ist ja tatsächlich so tipp topp in Ordnung, wie beschrieben. Dann ist alles OK.“. Auf meine etwas verwunderte Frage „das war alles?“ gingen wir ins Büro und er übergab mir die mitgebrachten Dokumente mit einem persönlichen Anschreiben an mich incl. Briefkopf, zugehöriger Umsatzsteuer-Identnummer und Gewerbeanmeldung bei der Limburgschen Handelskammer. Wir

vereinbarten, dass der Wagen am gleichen Tag von mir abgemeldet würde und zwischen 16.00 und 17.00 zur Abholung bereit stünde und dann der vereinbarte Preis in bar bezahlt würde.

Die Papiere sahen recht plausibel aus, aber mein Bauchgefühl (und darauf kann ich mich immer verlassen) sagte mir, dass da etwas nicht stimmte. Die Besichtigung war viel zu kurz gewesen und die Papiere waren so vertrauensbildend angelegt, dass es schon wieder verdächtig war. Meine größte Sorge lag darin, dass ich mir nicht zutraute, gut gemachtes Falschgeld bei der Übergabe von echtem unterscheiden zu können. Daher wäre mir eine Übergabe Zug um Zug z.B. mit gemeinsamem Einzahlen des Betrages bei einer Bankfiliale natürlich lieber gewesen. Mein Angebot, den Wagen sogar angemeldet nach Heerlen zu bringen und danach erst abzumelden, lehnte der Mann dankend ab.

Ich überprüfte also die Angaben mittels Online-Abfrage in Saarlouis und erhielt die Bestätigung, dass die Umsatzsteuer-Identnummer gültig war und zu dem beschriebenen Unternehmen mit der angegebenen Adresse passte. Jetzt hätte wahrscheinlich jeder gesagt, „also ist doch alles in Ordnung!“. (Merke: 3. Solche Angaben kann man sehr leicht selbst über das Internet ermitteln und auf ein Blatt Papier als Briefkopf schreiben. Dass es die Firma gibt und auch die Steuernummer passt, bedeutete ja nicht, dass der Käufer tatsächlich von der Firma legitimiert ist).

Ich meldete also das Fahrzeug beim StVA ab und fuhr zurück zum Büro. Wie zur Entkräftung meiner Bedenken rief dann auch Herr van den Haag noch einmal an und bestätigte den Abholtermin für den Nachmittag: „Das Auto ist ja wirklich topp und ich verspreche Ihnen, dass meine Kollegen sicher zwischen 16.00 und 17.00 Uhr bei Ihnen sind“.

Mir ließ das trotzdem keine Ruhe und ich begann, die Angaben auf dem Briefkopf der Reihe nach zu überprüfen. Die dort genannte Firma gab es tatsächlich und sie präsentierte sich im Internet mit aufwändigen Webseiten und verschiedenen, großen Standorten in Limburg. Nur Telefonnummer und Emailadresse passten nicht zu den Angaben auf dem Briefkopf. Auch fehlte dort die übliche Bankverbindung. Ich beschloss, unter einem Vorwand

über die im Internet angegebene Telefonnummer nach Herr van den Haag zu fragen, um zu überprüfen, ob es den dort wirklich gab, da ich zu dem Namen van den Haag und der Handynummer keine Verweise fand. Meine Verwunderung war recht groß, als ich erfuhr, dass Herr van den Haag in Urlaub sei. Das Angebot, mit einem Kollegen zu sprechen, nahm ich gerne an und erfuhr von dem verdutzten Kollegen, dass er die komplette Urlaubsvertretung machen würde und nichts von einem derartigen Ankauf wüsste. Ich faxte ihm die Seite zu und der Mitarbeiter des Autohauses sagte, dass er die angegebene Handynummer nicht kennen würde. Er versprach einen Rückruf. Kurze Zeit später meldete er sich zurück und teilte mir mit, dass sich unter der Handynummer nur eine Mailbox melden würde und die Stimme definitiv nicht die von Herrn van den Haag sei. Diesen hätte er auf seiner richtigen Mobilnummer erreicht und er wüsste nichts von dem Deal. Man würde jetzt mit der Geschäftsführung beraten, ob Anzeige erstattet würde, denn da würde offenbar jemand unter deren guten Namen Geschäfte machen wollen.

Ich rief dann bei der Kriminal-Polizei in Aachen an und wurde mit dem zuständigen Betrugsdezernat verbunden. Es dauerte etwas, bis ich die Beamten davon überzeugt hatte, dass Handlungsbedarf bestand, denn nach deren Auffassung war ja noch keine Straftat begangen worden. Den Ratschlag „Warten Sie mal, ob die kommen und rufen sie uns dann an“ war mir zu heikel und nachdem wir geklärt hatten, dass da offenbar mindestens eine Urkundenfälschung vorlag, versprachen die Beamten die Sache näher zu verfolgen. Nachdem ich dann in einem weiteren Telefonat mit der echten, holländischen Auto-Firma den obersten Chef persönlich am Apparat hatte, kam etwas mehr Licht in die Sache: „Das sind zwar unsere Firmenangaben, aber nicht unsere Email-Adresse, nicht unsere Telefonnummer und das ist nicht die Unterschrift von Herrn van den Haag, denn der steht mittlerweile hier neben mir!“, war die Aussage des Geschäftsführers. Der echte Herr van den Haag hatte sich auf dem Rückweg aus dem Urlaub befunden und war direkt in die Chefetage zitiert worden.

Das war jetzt für die deutsche Kripo der Auslöser zu handeln, denn entweder sollte jetzt ein Steuerbetrug (Umsatzsteuer), eine Kaufabwicklung mit Falschgeld oder einem ungedeckten Scheck oder

gar der Diebstahl des Fahrzeugs (quasi auf Bestellung) erfolgen. Mit Nachbarschaftshilfe parkten wir das Objekt der Begierde also erst einmal bis zum Eintreffen der Polizei zu. Insgesamt vier Kripobeamte (natürlich in Zivil) schlugen dann nach Mittag in meinem Büro auf und wir erörterten bei einer Tasse Kaffee die Sachlage und das mögliche Motiv. Zwei Polizeibeamte postierten sich unauffällig auf dem Parkplatz in der Nähe des zu verkaufenden oder zu stehlenden Fahrzeugs, während die zwei anderen bei uns im Büro auf die Täter warteten und die Fahndung mit den niederländischen Kollegen koordinierten.

Während ich auf eine Bezahlung per Falschgeld oder eine Steuerhinterziehung zu Ungunsten der richtigen Autofirma oder mir tippte, war der Favorit der Kripo zunächst ein Scheckbetrug nach folgender Masche:

Ein Käufer reagiert auf eine Internet-Anzeige und akzeptiert ohne große Verhandlung und ohne Besichtigung des angegebenen Preis. Dann wird ein Scheck per Post geschickt, der z.B. 2000,- € über den vereinbarten Betrag liegt. Der Käufer soll dann den Scheck einlösen und den überzähligen Betrag an einen angeblichen Spediteur überweisen, der dann das Fahrzeug abholt und exportiert. Löst der Käufer den Scheck dann tatsächlich ein, so wird dieser auch zunächst dem Konto gutgeschrieben. Der Käufer überweist dann die 2000,- € auf ein ausländisches Konto (meist per Bargeldtransfer zur Western Union) und wenn dann der Scheck wenige Tage später platzt und zurückgebucht wird, ist das überwiesene Geld längst anonym abgehoben worden. Vor dieser Masche wird übrigens ausführlich in den Sicherheitshinweisen bei mobile.de und bei der Postbank gewarnt. Das System des Bargeldtransfers über das Netz der Western Union dient zum schnellen Überweisen von Bargeld in Notfällen (auch bekannt als Postbank-Minuten-Service). Jeder, der die wichtigsten Daten der Transaktion kennt (Empfänger, Absender, Land und Höhe der Überweisung) kann bei jeder beliebigen Filiale der Western Union Bank weltweit das Geld in Bar abheben. In der Regel wird übrigens das Auto nie abgeholt. Das ist dann für den Geschädigten noch ein Trost, denn im schlimmsten Fall ist auch noch das Auto weg!

Aber zurück zu unserem Fall: Nach Rücksprache mit den holländischen Kollegen ergab sich ein anderes Motiv. Auf PKW wird bei der Einfuhr nach Holland eine Luxussteuer von 45% erhoben. Dadurch sind vergleichbare Fahrzeuge, die in Deutschland für 11.000 bis 13.000 € gehandelt werden in den Niederlanden erst ab 19.000 Euro zu haben. Vermutlich wollte der Betrüger also den Wagen in Holland unter Umgehung der Einfuhrsteuer weiterverkaufen und sich möglicherweise als mobiler Verkäufer der nachprüfbar existierenden Autofirma ausgeben. Der holländische Käufer hätte sich dann bei Problemen oder Steuerforderungen des holländischen Staates an die richtige Autofirma gewandt und vermutlich erfahren, dass Herr van den Haag gar nicht mit Legitimation gehandelt hätte. Geschädigt würden also je nach Konstellation die holländische Firma, der Endabnehmer und ggfs. ich als Verkäufer, da das deutsche Finanzamt letztlich von mir die Entrichtung der Umsatzsteuer gefordert hätte.

Aber alternativ zu diesem Szenario bestand natürlich auch die Gefahr, dass die Täter gar nicht zum vereinbarten Zeitpunkt auftauchen würden, sondern letztlich auf diese Weise nur der Standort eines nach Wunsch ausgestatteten Fahrzeugs und dessen Zustand ausgekundschaftet werden sollte um das Fahrzeug dann in der Nacht oder am Wochenende zu entwenden. Leider war unser Warten dann vergebens. Die Täter sind nicht mehr aufgetaucht und Herr van den Haag ist seitdem auch nicht mehr telefonisch erreichbar gewesen. Möglicherweise ist er durch einen Insider in der Autofirma gewarnt worden, denn der Inhaber des Autohauses hat die Vermutung geäußert, dass die Stimme an der Mailbox bekannt wäre. Nun fahndet die holländische und deutsche Polizei nach Herrn van den Haag. Das Fahrzeug wurde mit Polizeieskorte (kein Scherz) zu einer sicheren Unterkunft verbracht und wartet nun auf den Verkauf an einen ehrlichen Käufer.

Für den Ausgang der Geschichte, wäre es natürlich schön gewesen, ihnen jetzt auch schon den Täter samt tatsächlichem Motiv liefern zu können, aber das kann noch kommen. Für mich ist es so erst einmal besser, denn damit hielt sich der Schaden mit einem mehr oder weniger verlorenen Arbeitstag und 5,90€ Abmeldegebühr in Grenzen. Mein Bauchgefühl hat mich mal wieder gerettet! Mobi-

le.de nennt übrigens noch einige weitere mögliche Gefahren, die in direktem Zusammenhang mit Kaufofferten über das Internet stehen: So wird im Einzelnen davor gewarnt, Dokumente auch vorab per Email zu versenden, da die Verwertung der Angaben kriminellen Zwecke dienen kann. Probefahrten nie alleine durchführen lassen und Fahrzeugdokumente wie Kfz-Brief dann nicht mitführen. Vorsicht auch bei teuren Rückrufnummern als Antwort auf eine Kaufanfrage oder dem Kleingedrucktem im Kaufvertrag, nach dem der Kaufpreis von einem Gutachten abhängig gemacht wird, welches dann natürlich viel zu niedrig ausfällt. Auch vor der Aufnahme in so genannten Exportlisten wird gewarnt. Hier kommt nachher statt der Zusendung von kostenlosem Infomaterial ein kostenpflichtiger Vertrag in Höhe von 70,- € zustande.

Schlüssel verloren?

Ist Ihnen bewusst, dass auf Ihrem Notebook neben den darauf gespeicherten persönlichen und ggfs. vertraulichen Daten u.U. auch die Schlüssel zu Ihrem Büro oder Ihrem Heimnetz schlummern? Was ist, wenn das Notebook gestohlen wird? Tauschen Sie dann auch Ihre Schlösser aus?

Es ist in der heutigen Zeit technisch kein Problem mehr, sich mit einem Notebook per WLAN, VPN oder Fernwartungszugriff in das eigene Firmen- oder Heimnetzwerk einzuwählen. Die Zugangsinformationen sind dabei (weil das so praktisch ist) auf dem Notebook hinterlegt und erlauben so den automatischen Verbindungsaufbau zu den im Netzwerk gespeicherten, sensiblen Daten. Sollte Ihr Notebook verloren gehen oder gestohlen werden (und das passiert häufiger, als man denkt), so sind die auf dem Notebook gespeicherten Daten und Zugänge in Gefahr. Mittels geeigneter Programme lassen sich die Passwörter zurücksetzen, umgehen oder durch so genannte Brute-Force-Attacken durch automatisiertes Ausprobieren binnen Minuten oder Stunden herausfinden.

Sind dann z.B. Login-Daten zur Benutzeranmeldung an den heimischen Server oder das Email-Konto auf der Festplatte des Notebooks abgespeichert, hat der Dieb schnell Zugriff auf diese Daten. Im Falle des Falles, wenn also das Notebook gestohlen oder verloren wurde, müssen systematisch alle Zugangspasswörter und Benutzer-Accounts,

die sich möglicherweise auf dem Gerät befunden haben, umgehend geändert werden. Das entspricht dem Verfahren, was man typischerweise anwendet, wenn ein wichtiger Hausschlüssel verloren gegangen ist: Man tauscht die Schlösser aus.

Mittlerweile gibt es Sicherungen für Notebooks auf Hard- oder Softwarebasis, die es einem Dieb unmöglich machen sollen, die Daten zu verwerten, bzw. es erlauben, ihn aufzuspüren. Im letzteren Fall sorgt ein versteckt in dem System installierter Mechanismus dafür, dass bei jeder Online-Verbindung des Notebooks die Verbindungsdaten an einer vordefinierten Stelle abgelegt werden. Im günstigsten Fall kann man so den Standort des Notebooks anhand von Telefondaten oder Netzwerkadresse zurückverfolgen. Eine Methode zu mehr Datenschutz, die schon an "James Bond" oder „Cobra – übernehmen sie!“ erinnert, sind mit Chemikalienladungen präparierte Notebookfestplatten, die per Handyanruf gezündet werden und die Magnetoberflächen der Festplatte zerstören. Der Dieb würde in einem solchen Fall also keine Freude an den Daten des Notebooks haben. Sicherlich spektakulär und nur für extrem sicherheitsrelevante Daten von Interesse. Etwas weniger aufwändige Sicherungssysteme begnügen sich mit der Verschlüsselung der Festplattendaten (z.B. auf Basis des Windows eigenen EFS⁵ oder kombinierten Dongle/Token-Lösungen). Grundsätzlich sollte man jedoch beachten, dass eine solche Verschlüsselung nicht ohne Risiko zu haben ist. Im Fehlerfall oder bei Verlust des Schlüssels ist man u.U. selber nicht mehr in der Lage, die Daten noch einmal auszulesen. Regelmäßige unverschlüsselte Backups auf sicher verwahrte Medien sind daher ein Muss!

Schutzmechanismen

„Gefahr erkannt – Gefahr gebannt“ so beschreibt der Volksmund den ersten Schritt zu mehr Sicherheit. Ist erst einmal eine gewisse Sensibilisierung für den Datenschutz bei den Betroffenen erreicht, so sind konkrete Schritte zu mehr Datensicherheit nicht mehr weit entfernt.

Als Konsequenz der beschriebenen und bekannten Bedrohungs-Szenarien ergibt sich folgende Liste mit Sicherheits-Tipps:

1. Schränken Sie den lokalen, physikalischen Zugriff auf das EDV System so weit ein, dass kein Unbefugter direkten Zugang zum System erhält (Verwendung von nicht leeren, nicht trivialen Passwörtern, Aktivierung von Bildschirmschonern mit Kennwortschutz)
2. Schränken Sie die Zugriffsrechte auf Daten entsprechend der benötigten Nutzung ein. Arbeiten Sie im Normalfall nicht mit Administratorrechten.
3. Sorgen Sie für einen durchgängigen Virenschutz incl. regelmäßigen Virensignatur-Updates für alle Rechner (Server und Clients)
4. Aktualisieren Sie die Betriebssysteme der Computer (Patches, Service Packs)
5. Nutzen Sie eine Netzwerk-Firewall, die zwischen Netzwerk und Online-Zugang geschaltet und von einem Fachmann konfiguriert und gewartet wird (Personal-Firewalls auf Desktop-Ebene allein sind als Schutzmechanismus weitestgehend wirkungslos)
6. Lassen Sie Ihr System in regelmäßigen Abständen von Fachleuten auf Sicherheitsmängel überprüfen
7. Geben Sie keine Passwörter, Zugangskennungen oder TAN-Listen nach außen in fremde Hände und versenden Sie keine vertraulichen Informationen und Passwörter unverschlüsselt per Email
8. Verlangen Sie für rechtsichere Online-Kommunikation die digitale Signierung von Nachrichten durch den Sender.
9. Seien Sie skeptisch bei der Eingabe von personenbezogenen Daten auf Webseiten, die Sie nicht zweifelsfrei als authentisch identifizieren können oder auf die Sie per Email zur Eingabe von Benutzerdaten aufgefordert werden
10. Und zu guter letzt: Die Intelligenz sitzt vor dem Computer! Der PC ist nichts anderes als ein leistungsfähiges Werkzeug. Erlernen Sie die Handhabung und reagieren mit offenen Augen auf Informationen und Abfragen, die Ihnen die EDV liefert. Seien Sie gegenüber unverlangt eingegangenen Nachrichten skeptisch und misstrauisch und vergewissern Sie sich lieber einmal zu viel als zu wenig, ob die Information authentisch ist

⁵ Encrypting File System in Windows XP und Windows Server 2003

Fazit

Sollte man daher von Internetgeschäften Abstand nehmen oder das Medium als Hexenwerk verteuern? Meiner Meinung nach nein: Die Vorteile der Nutzung überwiegen bei weitem deren Risiken, wohlgemerkt bei intelligenter Nutzung dieser Kommunikationsform. Machen Sie es wie die Bewohner des alten Carcassone: Bauen Sie sich Ihre Festung und lassen Sie nur diejenigen herein, denen Sie vertrauen. Wir helfen Ihnen bei der technischen Umsetzung. Nutzen Sie dazu die individuelle Beratung oder gleich unser Pauschalangebot **IT-Security-Check**:

Durch systematische Analyse Ihrer Computeranlage werden Schwachstellen hinsichtlich typischer Bedrohungsszenarien aufgedeckt und konkrete Lösungen und Schutzmassnahmen erörtert und installiert. Durch günstige Pauschalpakete wird dieser Service für Sie kalkulierbar und macht sich binnen kürzester Zeit bezahlt – egal ob eine konkrete Bedrohungssituation gerade vorliegt oder für die Zukunft abgewehrt werden soll.

Unser Angebot

Bei unserem IT-Check überprüfen wir Ihre Systeme nicht nur hinsichtlich sicherheits-relevanter Punkte, wie z.B. dem Virenschutz, Dialer-Schutz, Erkennen und Aufspüren von Trojanern und Spionage-Software (Spyware und Backdoor-Software), sondern betrachten Ihre EDV ganzheitlich. Daher wird auch überprüft, ob Sie ein funktionierendes und schlüssiges Backup-Konzept zur Datensicherung haben und ob Passwörter und Zugangsberechtigung nach heutigen Maßstäben fachmännisch umgesetzt werden. Egal ob Ihre EDV aus einem einzigen PC oder einem Netzwerk mit Wireless-LAN, Firewall, VPN usw. besteht, wir machen Ihre Systeme fit gegen die üblichen Bedrohungen von innen und außen und schulen Sie im Hinblick auf den sicheren Umgang mit dem leistungsfähigen, aber auch sensiblen Werkzeug „Computer“.

Gleichzeitig mit der Sicherheitsbetrachtung wird Ihr PC auch im Bereich der Systemstabilität verbessert, optimiert und von unnötigem Ballast befreit.

Die abschließende Ergebniszusammenfassung und die daraus resultierende Beratung wird Ihnen wichtige Aussagen liefern, ob Ihre EDV nun als „sicher“ zu betrachten ist oder welche Schritte notwendig sind, um akute oder mögliche Bedrohungen zu verhindern bzw. in ihrer zerstörerischen Wirkung zu minimieren.

Leistungsumfang IT-Check

Das Basispaket beinhaltet die Abarbeitung folgender Kernpunkte (pro PC werden rund 100 verschiedener Punkte überprüft):

- Überprüfung des PCs auf Viren incl. Update der Virensignaturen (ggf. zzgl. entsprechender Virenschutzsoftware oder einer Abo-Verlängerung, falls Software nicht vorhanden)
- Suche nach Spyware, Trojanern, Würmern, Backdoor- und Dialer Programmen incl. deren Entfernung
- Systemoptimierung auf BIOS- und Betriebssystemebene u.a. durch entfernen nicht benötigter Dateien und Software
- Aktualisierung der Betriebssystem-Software (Servicepacks)
- Überprüfung und ggf. Installation des SPAM-Schutzes (ggf. zzgl. entsprechender Antispam-Software oder einer Abo-Verlängerung, falls Software nicht vorhanden)
- Überprüfung und ggf. Optimierung von Backup- und Passwortkonzepten
- Analyse von Ereignisprotokollen und Optimierung des Startverhaltens (residente Programme)
- Hinweis auf erkannte Schwachstellen und Beantwortung von Anwenderfragen zum Thema IT-Sicherheit
- Zusammenfassung der Ergebnisse und Beratung hinsichtlich möglicher Optimierungen

Preise

Im Basispaket ist die An- und Abfahrt im Raum von 25 km ab Aachen-Jülicherstrasse/Zentrum sowie die Untersuchung des ersten PCs im Netzwerk (Einzelplatz oder Server-PC) enthalten.

Paketpreis für den 1. PC: 199,- € incl. MwSt.

(zusätzliche km incl. Fahrtzeit über diesen Radius hinaus: 1,99 €/km für Hin- und Rückfahrt)

Jeder weitere zu untersuchende PC wird zum Pauschalpreis von **49,- € incl. MwSt.** überprüft und optimiert.

Ist eine **Firewall auf Paket-Filter-Basis** im Netzwerk vorhanden und auf Funktion und Konfiguration zu überprüfen, so wird hierfür ein Aufpreis von **99,- € incl. MwSt.** erhoben.

Ein ggf. vorhandenes **Funk-Netzwerk** (Wireless LAN) wird für **49,- € incl. MwSt.** auf dessen sichere Konfiguration (Verschlüsselung, Authentifizierung, Passwörter etc.) überprüft und ggf. optimiert.

Alternativ rechnen wir auf Ihren Wunsch auch nach tatsächlichem Aufwand ab. Dies bietet sich vor allem dann an, wenn zusätzliche Servicearbeiten außer dem IT-Check anstehen oder Sie eine speziellere IT-Infrastruktur im Einsatz und besondere Aufgabenstellungen haben.

Interesse geweckt?

Warten Sie nicht, bis es zu spät ist! Der nächste Virus kommt bestimmt!

Investieren Sie in Ihre EDV-Sicherheit!

Wir dürfen uns als langjährigen und kompetenten Partner der EDV Anwender empfehlen und freuen uns auf Ihren Auftrag:

Tel. 0241/96877-0



Unser Motto: Ihr EDV Problem ist unsere Aufgabenstellung. Sollten Sie Opfer eines sicherheitsrelevanten EDV-Vorkommnis geworden sein und hier konkreten Beratungs- bzw. Analysebedarf haben, so darf ich mich in meiner Eigenschaft als EDV-Sachverständiger empfehlen. Ob Beweissicherung oder die Aufstellung eines Incident Response-Planes: Rufen Sie an!

Ihr Thomas Käfer (Dipl.-Ing. Informationsverarbeitung und EDV Sachverständiger)

Neue Produkte – Kurz notiert



Twin Micro Saver

Zum Schutz von Notebook und Beamer

Sichert die Geräte mit so genanntem Kensington Lock mit einem 1,80 m langen Stahlkabel und 3-Zahlen Kombinationsschloss.

Preis 69,- € incl. MwSt für zwei Geräte

Preis 49,- € incl. MwSt für ein Gerät



Travel Plug Adapter

Internationaler, kompakter Steckeradapter für die Reise - Kann in über 150 Ländern verwendet werden. Einfach den benötigten Stecker herausziehen und schon können Sie auch unterwegs die Steckdose schnell nutzen.

Preis: 19,- € incl. MwSt.

HP iPAQ rz1710 - Navigator



Beim HP iPAQ rz 1710 Navigator handelt es sich um ein komplettes GPS-Navigationssystem zum Einbau in Fahrzeuge, das einfach, kostengünstig und sofort einsetzbar ist. Dieses handliche Gerät passt perfekt in jedes Fahrzeug und lässt sich problemlos von einem Fahrzeug in ein anderes umsetzen. Somit steht eine ultimative "Plug & Drive"-Lösung zur Verfügung. Das Gerät ist mit der neuesten Navigationssoftware ausgestattet, um visuell und per Sprachführung auf Fahrtrichtungsänderungen hinzuweisen und eine innovative Benutzeroberfläche mit Ode-Touch-Funktionalität bereitzustellen

- Einfach zu installieren und zu verwenden
- Handlich - unabhängig davon, wohin und wie Sie reisen
- Perfekte Integration in Fahrzeuge
- Zuverlässig und effizient
- Komplettpaket 399,- incl. MwSt

Labtec Notebook Maus



Kabellose optische Notebookmaus mit Mini Empfänger auf 2,4 GHz-Basis. Ideal für unterwegs. Der Mini-Empfänger passt zur Aufbewahrung ins Innere der Maus.

Preis 29,-€ incl. MwSt.



CHIPDRIVE® Zeiterfassung

Mehr als 30.000 kleine und mittelständische Unternehmen setzen die preisgünstige und praktische Lösung bereits ein, um die Arbeitszeiten ihrer Mitarbeiter zu erfassen.

Als fälschungssicheres Medium ordnen Sie die Chipkarte einem Mitarbeiter fest zu, der sie dann einfach wie eine Stempelkarte verwendet. Als Stempelgerät dient ein kleiner, mobiler Chipkartenleser, der alle Daten zwischenspeichert. Die zugehörige umfangreiche Software sorgt für die Kontrolle und Analyse der Daten: Urlaub, Gleitzeit, Fehlzeiten, Zeitpläne für Projekte und Sonderregelungen – Sie haben alle Zeiten immer im Griff!



Unser Starterkit enthält alle nötigen

Module für 25 Mitarbeiter, vom mobilen Chipkartenleser über die Software bis zu den benötigten



Chipkarten. Oder aber, Sie stellen sich Ihre Lösung individuell zusammen, denn jedes Modul bieten wir auch einzeln an. So können Sie CHIPDRIVE® Zeiterfassung beliebig erweitern.

Preis Starterkit 389,- € incl. MwSt. (ohne Installation)

Wireless Accessory Kit für Notebooks

Wireless Accessory Kit - Kompakte Maus und Nummern-Pad für Notebook. Kabelloser Mini-USB-Empfänger. Optische Maus mit 800dpi Auflösung. Praktischer Ein-/Ausschalter spart Batterien.

Preis 39,- € incl. MwSt.





Vodafone Mobile ConnectCard UMTS

E-Mails checken, online gehen, aufs Firmennetz zugreifen - mit einer Vodafone Mobile ConnectCard UMTS nutzen Sie unterwegs den Komfort eines Highspeed-Büros. Denn mit dem Übertragungsstandard UMTS (Universal Mobile Telecommunications System) lassen sich rasante Verbindungen mit bis zu 384 KBit/s aufbauen. Ideal, wenn Sie sich häufig in Ballungszentren aufhalten.

Zusätzlich eignet sich die Datenkarte fürs Notebook auch für GPRS-Verbindungen. So profitieren Sie auch außerhalb der UMTS-Versorgungsgebiete dank der Vodafone-GPRS HighPerformance-Technologie von sehr schnellen Datenverbindungen.

Auch bei uns für 1,-€* !

***Verkaufspreis 199,- € incl. MwSt. Bei Abschluss des obligatorischen Vodafone Vertrages zur Nutzung der Karte erhalten Sie ein Guthaben von 198,- € als Gutschrift auf einer der ersten Rechnungen durch Vodafone.**

Elmeg Systemtelefone ISDN und VOIP



Abbildung ähnlich

Mit dem neuen IP-Systemtelefon elmeg IP-S290 und dem Modul VoIP-VPN Gateway wird die komfortable elmeg-Systemtelefonie jetzt auch in IP-Netzen verfügbar. Als Schnittstellen-Variante des elmeg CS290 unterstützt das elmeg IP-S290 alle System-Leistungsmerkmale an den ITK-Systemen der Reihe elmeg ICT wie Makeln, Vermitteln, Dreierkonferenz, Teamfunktionen, Linien-/Leitungstasten, Zugriff auf das anlageninterne

alphanumerische Telefonbuch und Vieles mehr. Integrieren Sie Systemtelefonie einfach in Ihr LAN- ein Ethernet-Anschluss ermöglicht einfaches Einstecken des Telefons in die nächste verfügbare Netzwerkbuchse. Damit entfällt auch der Administrationsaufwand, der bei internen ISDN-Leitungen notwendig ist – eine exakte Adressierung von Rufen an das Telefon wird über das LAN automatisch hergestellt, egal über welche LAN-Buchse das Telefon verbunden ist.

Preis 149,- € incl. MwSt. oder als ISDN Systemtelefon CS410 199,- € incl. MwSt

Machen Sie Ihr TFT-Display flexibel:

Ergotron bietet Ihnen eine umfangreiche Produktpalette von Montage-lösungen für ein breites Spektrum von Flachbildschirmen und deren Peripheriegeräten.



Das Sortiment umfasst Wandhalterungen, TFT-Schwenkarme mit Höhenverstellung bzw. Teleskopfunktion, Mehrschirmlösungen, Computerrahmen sowie Tastaturhalterungen. Ergotron platziert Ihre Hardware-Komponenten dort, wo sie benötigt werden. Nutzen Sie unsere reichhaltigen Erfahrungen aus den verschiedenen Marktsegmenten und das damit verbundene Know-how in der effizienten und ergonomischen Arbeitsplatzgestaltung - Angenehmes Arbeiten mit TFT Monitoren und gleichzeitig mehr Arbeitsfläche nutzen. Der Neo-Flex ist praktisch für alle TFT-Monitore geeignet, und in weniger als 5 Minuten an Ihrem Schreibtisch zu montieren.

Preis ab 115,- € incl. MwSt.

