softScheck
we identify vulnerabilities others don't

Aufpassen wenn ...

Eine kleine Einführung in die Informationssicherheit für Private und kleine Unternehmen

Stand: 1. August 2011

Prof. Dr. Hartmut Pohl
Geschäftsführender Gesellschafter softScheck GmbH Köln
Hartmut.Pohl@softScheck.com
www.softScheck.com

softScheck
we identify vulnerabilities others don't

Aufpassen, wenn …

Eine kleine Einführung in die Informationssicherheit
für Private und kleine Unternehmen

Aufpassen wenn,

I. ein Mitarbeiter ausscheidet
II. ein neuer Mitarbeiter kommt
III. nichts passiert …
IV. Hacker aktiv sind – oder sind es Innentäter?
V. Sie mit e–Mails arbeiten
VI. ein Virus auftaucht
VII. Daten verloren sind: Backup
VIII. Ihre Software veraltet: Patches
IX. Ihr PC kontrolliert werden muss

Diese Broschüre stellt die überarbeitete Fassung einer in der Zeitschrift Impulse abgedruckten Artikelfolge dar; der Autor dankt den Herausgebern für die Unterstützung ganz herzlich.

Prof. Dr. Hartmut Pohl

Geschäftsführender Gesellschafter softScheck GmbH, Köln

www.softScheck.com

phone: +49 (2241) 955 88 – 81
fax: +49 (2241) 955 88 – 89
Hartmut.Pohl@softScheck.com

Registergericht: Amtsgericht Köln HRB 72534

Köln 2011

Aufpassen, wenn ein Mitarbeiter ausscheidet

Stillstand der Produktion, Wirtschaftsspionage und Sabotageakte, Ausfall der Informationstechnik (IT) in Ihrem Unternehmen – und Sie wissen nicht warum? Erst eklatante Störfälle machen uns klar, wie abhängig wir von der Informationstechnik sind zur Aufrechterhaltung der Produktion und bei der Kommunikation mit Auftraggebern und Zulieferern über das unsichere Internet.

Im ersten Halbjahr 2002 haben die Fälle von Computerspionage und Computersabotage überproportional stark zugenommenen. Täter sind nicht irgendwelche ominösen Hacker. Täter schadensträchtiger Spionagefälle oder Sabotageakte sind eigene Mitarbeiter (!) – auch frühere Mitarbeiter – oder mit Insiderwissen gespickte Außenstehende – auch Ihrer Auftraggeber und Zulieferer.

Ehemalige Mitarbeiter kennen (noch) die gesamte IT und Ihr Netzwerk, kennen die Sicherheitsmaßnahmen, die Passworte und – die ehemaligen Kollegen.

Folgende Sicherheitsmaßnahmen sind unverzichtbar, wenn ein Mitarbeiter ausscheidet (Kündigung).

- Wenn ein Mitarbeiter kündigt, lassen Sie ihm sofort alle (!) Zugriffsrechte nehmen: Passwörter müssen unverzüglich gelöscht – bzw. abgeändert werden. Er darf dann danach keine wertvollen Daten mehr versenden oder auf Datenträger kopieren. Kündigen Sie, so lassen Sie ihm die Rechte zeitgleich mit dem Abschlussgespräch nehmen.
- Lassen Sie ihn mit sofortiger Wirkung von allen Pflichten freistellen – und nehmen Sie ihm alle Rechte.
- Der Ausscheidende wird wahrscheinlich auch Passworte von Kollegen (zufällig) gehört oder gesehen haben. Alle Mitarbeiter, deren Passwort er auch nur kennen könnte, müssen ihr Passwort sofort ändern.
- Auch für die Passworte von Servern und Dateien, die der Mitarbeiter benutzt oder gesehen haben könnte, müssen sofort geändert werden – im Zweifel müssen also alle Passworte des Unternehmens geändert werden.
- Lassen Sie ihn nach dem Kündigungsgespräch von einem verantwortungsvollen Mitarbeiter sofort zum Schreibtisch begleiten und unter Kontrolle alle seine erkennbar privaten Dinge mitnehmen – aber keinesfalls mehr! Achten Sie besonders auf Datenträger wie Disketten, CDs, Streamer–Bänder.
- Lassen Sie ihn alle seine Arbeiten, seine Arbeitsnotizen an seinen Vorgesetzten übergeben und kontrollieren Sie die Übergabe.
- Lassen Sie ihn Ihr Unternehmen nur noch mit Ihrer ausdrücklichen Genehmigung betreten – auch die Zweigstellen.
- Informieren Sie unverzüglich alle Mitarbeiter über das Ausscheiden und sensibilisieren Sie alle über die möglichen Risiken und Sicherheitsaspekte.
- Überprüfen Sie alle unternehmensspezifischen Auskünfte an den Ehemaligen. Lassen Sie sich über (versuchte) Besuche des Ehemaligen und auch über Anrufe und e–Mails informieren – auch über die Inhalte.

Alle diese Maßnahmen sind selbstverständlich. Je sicherheitsbewusster der Mitarbeiter ist, umso mehr und eher wird er die Maßnahmen verstehen. Informieren Sie alle Mitarbeiter über diese vorbeugenden Maßnahmen und begründen Sie diese auch – mit möglichem Know–How–Abfluss oder Sabotagemöglichkeiten – und machen Sie den Unterschied zur Bespitzelung deutlich.

Aufpassen, wenn ein neuer Mitarbeiter kommt

Ein neuer Mitarbeiter kennt Ihr Unternehmen nicht, er kennt nicht die formellen und erst recht nicht die informellen Regeln. Insbesondere kennt er nicht Ihre Sicherheitskultur. Sprechen Sie daher mit dem Neuen über Ihre Sicherheitsstrategie – und begründen Sie ihm gegenüber den Wert der Unternehmensinformationen und erläutern Sie ihm die Abhängigkeit Ihres Unternehmens von der Informationstechnik (IT). Stellen Sie ihm die Folgen eines möglichen Stillstands der Produktion und eines möglichen Falls von Wirtschaftsspionage und von Sabotageakten dar anhand des wirtschaftlichen Schadens für Ihr Unternehmen und insbesondere für die Arbeitsplätze – auch für seinen. Stellen Sie ihm einen Kollegen als 'Paten' zur Seite, der ihm in allen sicherheitsrelevanten – insbesondere den technischen – Aspekten zur Seite steht und ihm die u.g. Regelungen erläutert und begründet.

Folgende Sicherheitsmaßnahmen sind bei Einstellungen unverzichtbar.

- Sensibilisieren Sie Ihren neuen Mitarbeiter für Informationssicherheit, indem Sie ihn darauf hinweisen, dass Ihr Unternehmen von dem erarbeiteten Know–How lebt und davon abhängig ist, dass dieses auch nicht an Mitbewerber gelangt! Stehen Sie ihm für Sicherheitsfragen grundsätzlicher Art auch persönlich zur Verfügung.
- Räumen Sie ihm Zugriffsrechte auf Daten und Programme ein, die er in der ersten Woche nutzen und anwenden muss. Die Zugriffsrechte sollten eine auf die erste Woche beschränkte Gültigkeitsdauer haben.
- Der Neue benötigt unverzichtbar sofort Zugriffsrechte, damit er nicht die Accounts von Kollegen benutzen muss. Kollegialerweise – aber entgegen jeder Sicherheitsrichtlinie – bieten gern freundliche Mitarbeiter dem Kollegen ihre Accounts und Passworte an – mit der Folge, dass der Neue die Passworte aller Kollegen kennt.
- Keinesfalls darf ein neuer Mitarbeiter bereits in der ersten Woche alle Zugriffsrechte erhalten, die er jemals im Unternehmen benötigen könnte – im Gegenteil sollten die Rechte sehr stark eingeschränkt sein. Insbesondere unternehmensvertrauliche Daten darf er nicht zur Kenntnis bekommen.
- Geben Sie ihm dazu ein Passwort, das ihn zu nichts weiter berechtigt als ein persönliches Passwort festzulegen (Einmal–Passwort). Dieses Passwort sollte dann eine Gültigkeitsdauer von einer Woche haben.
- Nach Bewährung des Mitarbeiters in der ersten Woche werden die Zugriffsrechte des Neuen zusammen mit seinem Passwort auf einen Monat verlängert. Danach werden die Rechte monatlich weiter verlängert bis zum Ende seiner Probezeit.
- Achten Sie darauf und befragen Sie den Neuen auch, ob er nicht etwa Daten seines früheren Arbeitgebers mitgenommen hat und in Ihr Unternehmen einbringen will! Sie machen sich sonst bei Wirtschaftsspionage mitschuldig.

Für Zeitmitarbeiter, Studenten in den Semesterferien o.ä. gelten diese Regeln für die gesamte Dauer der Tätigkeit!

- Erst nach Ablauf der Probezeit dürfen einem Mitarbeiter alle für die Ausübung seiner Funktion notwendigen Zugriffsrechte entsprechend seinen Zuständigkeiten übertragen werden. Dazu können dann auch Unternehmens–vertrauliche Daten gehören.
- Grundsätzlich dürfen Datenträger wie Disketten, CDs, Streamer–Bänder nicht aus dem Unternehmen mitgenommen werden – z.B. nach Hause.
- Informieren Sie alle Mitarbeiter über den Eintritt des Neuen ins Unternehmen zusammen mit seinen konkreten Aufgaben und Zuständigkeiten.
- Lassen Sie den Neuen in der Probezeit keine Urlaubs– oder Krankheitsvertretung übernehmen, die den Zugriff auf Unternehmens–vertrauliche Daten erfordern.

Achten Sie darauf, dass sich der Neue den korrekten Umgang mit Unternehmens–vertraulichen Daten einprägt und auch danach handelt. Dies gilt auch für Sicherheitsinformationen der IT. Unbegründete Neugier nach Passworten von Kollegen, Servern, Dateien sollte Misstrauen bei den Kollegen wecken. Lassen Sie sich persönlich über unbegründete Neugier auf Sicherheitsdetails informieren.

Aufpassen, wenn nichts passiert ...

Ihre Informationsverarbeitung/Informationstechnik (IT) läuft Tag und Nacht und auch am Wochenende einwandfrei? Ohne Probleme – eigentlich seit Jahren?

Tatsächlich haben längst immer wieder Mitbewerber unternehmenskritische Daten aus Ihrem Server kopiert, mehrfach war auch die SCM–Software in entscheidenden Situationen nicht verfügbar, so dass die Produktion unterbrochen werden musste. Nur keiner hat's gemerkt.

Wie schützen Sie sich denn überhaupt gegen heimliche Besuche auf Ihren Servern oder sogar Spionage und Sabotage durch Mitbewerber? Angriffe und daraus folgend Störfälle sind alltäglich. Folgende Sicherheitsmaßnahmen sind daher unverzichtbar.

- Lassen Sie ein Viren–Suchprogramm installieren und auch wirkungsvoll konfigurieren (Löschen gefundener Viren, Benachrichtigung an den Administrator). Achten Sie darauf, dass Sie mindestens täglich die aktuellen Virenkennzeichen ('Signaturen') vom Hersteller erhalten. Anderenfalls werden die jüngsten Viren nicht erkannt.
- Meist werden Viren über das Internet verteilt. Allerdings können sie auch über portable Datenträger wie Platten, Disketten, CDs und Streamer–Bänder o.ä. übertragen werden: Kontrollieren Sie daher alle eingehenden Datenträger auf Viren.
- Glauben Sie nicht, dass Sie einen Angreifer oder einen Virus ohne weiteres erkennen! Wenn Sie die Schadenswirkung des Virus bemerken, ist es jedenfalls zu spät. Sie müssen schon entsprechende Suchprogramme einsetzen.
- Manche Viren entfalten ihre Wirkung erst nach Wochen oder zu bestimmten Anlässen. Die Wirkungen sind auch sehr unterschiedlich: Ihre Daten werden gelöscht – ggf. auch 'nur' teilweise verändert oder gelöscht – dies erschwert Ihre Reparaturarbeiten maßlos, da Sie nicht sofort erkennen, welche Daten nun fehlen, welche 'nur' verändert wurden und welche noch korrekt sind.
- Lassen Sie eine sog. Firewall installieren, mit denen Sie nicht–benötigte Verbindungen ins Internet und aus dem Internet zu Ihnen ins Unternehmen verhindern.
- Lassen Sie ein Intrusion Detection System installieren. Dank gespeicherter Angriffsmuster erkennt es Angriffe auf Ihre Systeme.
- Lassen Sie ausschließlich Produkte installieren, die dem Stand der Technik entsprechen. Entscheidend ist die Konfigurierung der Systeme entsprechend den Anforderungen Ihres Unternehmens sowie die Auswertung der Protokolldaten.
- Beobachten Sie sorgfältig Ihre potentiellen Kunden, prüfen Sie, warum sie welche Aufträge nicht erhalten haben – hat evtl. ein Mitarbeiter Ihre Vorarbeiten und Entwicklungen schon längst ausspioniert und nun auch noch den angebotenen Preis? Informieren Sie sich also über die Produkte Ihrer Mitbewerber und die Preisgestaltung.
- Unverzichtbar ist eine mindestens tägliche (!) Sicherungskopie aller Daten: Programme, Netzwerkeinstellungen, Nutzdaten – und auch der eingesetzten Hardware und Software. Damit können Sie im Ernstfall (Brand, Wasserschaden, andere Katastrophen, Sabotage) Ihre Daten binnen einer oder weniger Stunden regenerieren. Lagern Sie eine aktuelle Kopie im Unternehmen, die ältere außerhalb (z.B. Filiale) und die älteste an einem sicheren Ort wie Banktresor. Archivieren Sie Ihre Geschäftsdaten.
- Informieren und sensibilisieren Sie alle Mitarbeiter für diese Risiken und Maßnahmen.

Aufpassen, wenn Hacker aktiv sind – oder sind es Innentäter?

Hacker, Cracker, Passwort–Knacker, Schüler und Studenten bevölkern das Internet und viele greifen Unternehmen und Behörden auch an. Sie knacken Passworte, lesen und ändern (!) Ihre Daten und verseuchen Ihre Rechner mit Viren und Würmern. Sind wir diesen Kids – oder besser gesagt Vandalen oder auch Chaoten – völlig ausgeliefert?

Nein, gegen diese meist zufälligen oder willkürlichen Angriffe helfen Firewalls, Virensuchprogramme und Zugriffskontrollen (Grundschutz). Damit wehren wir die meisten dieser Angriffe ab.

Gezielte Angriffe fahren die Kids allerdings kaum, schadensträchtige Angriffe fahren sie sehr selten. Warum? Sie wissen viel zu wenig über Ihr Unternehmen, Ihre Sicherheitsmaßnahmen, Ihre Netzstruktur etc. etc. Völlig falsch wäre es zu glauben, Angriffe und Manipulationen kämen ausschließlich von außen, dem Internet – eben von solchen Kids.

Tatsächlich werden die schadensträchtigen Spionagefälle und Sabotageakte weit überwiegend (bis hin zu 95 % aller Angriffe) von den eigenen (!) Mitarbeitern begangen. Oder von Außenstehenden, die gezielt von den eigenen Mitarbeitern über die Sicherheitsmaßnahmen informiert wurden – gelegentlich auch von Mitarbeitern, die gutgläubig oder fahrlässig derart wichtige Informationen weitergeben: Innentäter.

Und überhaupt: Wie sieht es denn mit Ihren Partnern aus, Ihren Auftraggebern und Ihren Zulieferern? Dürfen diese im Rahmen von Customer Relationship Management (CRM) oder Supply Chain Management (SCM) auf Ihre Server zugreifen? Ja, dürfen sie. Häufiger als uns lieb ist. Wissen Sie, wie hoch das Sicherheitsniveau Ihrer Partner ist? Wir können es nicht wissen und wir können es erst recht nicht kontrollieren – was kontinuierlich und dringend notwendig wäre.

Gegen alle diese Innentäter müssen wir uns schützen! Für sicherheitsbewusste Unternehmen sind also die folgenden Maßnahmen unverzichtbar.

- Restriktive Zugriffskontrolle: Jeder Mitarbeiter darf ausschließlich nur auf die Daten zugreifen, die er für seine Arbeit braucht. Lassen Sie diese Zugriffsrechte auf Korrektheit und Notwendigkeit überprüfen – regelmäßig.
- Lassen Sie alle Passworte in unregelmäßigen Abständen ändern. Lassen Sie regelmäßig auch die 'Qualität' der benutzten Passworte überprüfen – mindestens 6 Zeichen, möglichst 8, nicht nur Alphazeichen, sondern auch Ziffern und Sonderzeichen etc. Lassen Sie auch überprüfen, ob die Passworte überhaupt gewechselt wurden; manche Mitarbeiter wechseln gleich zweimal: Einmal zu einem schwierig zu merkenden und dann gleich wieder zurück zum alten Passwort.
- Lassen Sie die Protokolle vom Betriebssystem, Router, Firewall, Anwendungssoftware etc. ständig auswerten, um mögliche Fehlzugriffe oder sogar Angriffe erkennen zu können. Lassen Sie sich eine Zusammenfassung regelmäßig vortragen und bei Missbrauch oder auch nur wiederholten Fehlzugriffen sofort informieren.
- Sie können jegliche private Nutzung des Internet durch eine Betriebsvereinbarung unterbinden. Abgesehen von dem zeitlichen Aufwand fürs Surfen etc. entstehen Kosten für die Nutzung des Internet. Wenn Sie dies nicht für angemessen halten, lassen Sie gelegentlich die drei am häufigsten benutzten Web–Adressen feststellen. Hier haben schon manche Unternehmer 'Überraschungen' erlebt.
- Kontrollieren Sie alle Computer in unregelmäßigen Abständen auf Spiele (!), Bilder etc. etc. und auf evtl. eingespielte Viren.

Bringen Sie jeden strafrechtlichen Fall (Kinderpornografie etc.) sofort zur Anzeige. Informieren Sie alle Ihre Mitarbeiter über diese Konsequenzen von vornherein und machen Sie den Imageschaden deutlich, wenn Ihr Unternehmen wegen kriminellen Verhaltens auch nur eines einzigen Mitarbeiters in die Schlagzeilen gerät: Aufträge könnten storniert werden, Arbeitsplätze geraten in Gefahr ... Machen Sie in jedem Fall deutlich, warum Sie derart rigide bei Kriminalität vorgehen. Dies alles hat nichts mit Bespitzelung zu tun.

Aufpassen, wenn Sie mit e–Mails arbeiten

E–Mail ist derzeit das preiswerteste Kommunikationsmedium. E–Mails kosten nur einen Bruchteil von Cent 'Porto' und sind in Sekundenschnelle beim Empfänger. Gegenüber einem Telefongespräch hat eine e–Mail genauso wie ein Fax und der klassischer Brief den Vorteil, gelesen werden zu können, wann der Empfänger es will. Und Originaldokumente wie Angebote oder Preislisten können beliebig angehängt werden. Bei allen Vorteilen gibt es natürlich auch (vermeidbare) Risiken.

Das größte Risiko ist zweifellos das völlig unsichere Internet, in dem jedermann uneingeschränkt alles lesen kann. Ihre Adresse kann missbraucht werden, in dem sie an Werbeunternehmen verkauft wird. Wie alle Daten können auch Ihre e–Mails 'verloren' gehen – auf Ihrem eigenen Computer unabsichtlich gelöscht werden. Einfache Sicherheitsmaßnahmen helfen hier:

- Werbemails: Geben Sie Ihre e–Mail Adresse nicht in Chatrooms weiter, in Annoncedienste und andere unkontrollierbare Bereiche. Häufig genug werden dort die Adressen an Werbetreibende verkauft, die Ihnen anschließend 50 oder mehr Werbemails (sog. Spam) pro Tag von verschiedenen, wechselnden Absenderadressen zusenden – weltweit sind es heute 5 Milliarden Werbemails pro Tag. 3.5 Millionen solcher Adressen werden für einen Euro verkauft.

  Es ist sehr zeitaufwändig, die Mailbox auf Spam durchsehen und die Werbemails zu löschen. Achten Sie dabei besonders auf Mails ohne Bezug (subject), ohne erkennbaren Absender oder mit Ihrem Namen als Absender (!) oder auch ohne Inhalt – außer vielleicht einer Web–Adresse.

  Antworten Sie auf keinen Fall auf solche Werbemails. Der Absender erkennt an Ihrer Antwort, dass es sich um eine existierende Adresse handelt, deren Besitzer die eingehenden Mails sorgfältig liest. Gerade das will der Werbetreibende und Sie erhalten noch mehr Werbemails.

  Legen Sie eine spezielle Mailbox an für alle Mails, die Begriffe enthalten, mit denen Sie im Unternehmen nichts zu tun haben. Dazu werden meist alle Hilfsmittel gehören, die zur Vergrößerung oder auch Verkleinerung menschlicher Organe verkauft werden sowie alles, was mit Sex zu tun hat inklusive Medikamentenangebote. Weitverbreitet sind auch Angebote über die günstigsten Kredite seit 50 Jahren, Autoversicherungen und natürlich Angebote, die schönsten und interessantesten Frauen kennenzulernen ... Die meisten Mail–Programme enthalten unterstützende Filterfunktionen, um solche Mails auszufiltern, bevor Sie sie gesehen haben.

  Mit der Filterfunktion können Sie auch die Überflutung mit vielen Tausenden von Mails (Mail–bombs) von einem oder wenigen Absendern kanalisieren.

- Geldgeschäfte: Fallen Sie bloß nicht auf die finanziellen Probleme von angeblichen Afghanen, Irakern oder Nigerianern rein, die – unabhängig von ihrem aristokratischen Rang wie Prinz oder Bruder des Königs oder 3. Witwe des (früheren) Finanzministers – 50 oder 100 Mio. $ außer Landes bringen wollen und dazu ganz wenig Geld brauchen, um die Überweisungen bezahlen zu können oder Beamte zu schmieren.

  Oder Fonds zum Wiederaufbau zerstörter Krankenhäuser oder unter Denkmalschutz stehender historischer Denkmale oder ... Das sind seit vielen Jahren (sehr erfolgreich) praktizierte Betrugsversuche.

  Reagieren Sie überhaupt nicht auf alle Ihnen unbekannten Anbieter von Dienstleistungen oder Geschäften – es sei denn, Sie können sich anderweitig – z.B. durch einen Telefonanruf, Auskünfte anderer Geschäftspartner, Handelskammern o.ä. von der Seriosität des Senders überzeugen.

- Mailanhänge – Attachements: Viren sind bisher ausschließlich in Mail–Anhängen aufgetaucht. Öffnen Sie daher nie (!) den Anhang von Mails, ohne ihn auf Viren geprüft zu haben. Das gilt für ausführbare Dateien (.exe o.ä.) genauso wie für Text– oder Tabellendokumente.

- Schalten Sie dazu auch Optionen wie automatisches Öffnen des Anhangs Ihres Mail–Programms ab.
- Kettenbriefe: Reagieren Sie nicht auf Kettenmails, in denen vor neuen und alten Viren, Unglück, Krankheit o.ä. gewarnt, gebettelt oder auch einfach um eine Mail an eine bestimmte Adresse gebeten wird, zum Trost einer so sehr traurigen„ kranken Person oder auch nur um Weiterleitung an Ihre 10 besten Freunde. In vielen Mails wird mit 'heraufziehendem Unglück' gedroht, wenn Sie nicht den Anweisungen folgen. Alles Mumpitz (Hoax). Sie machen sich mit der Weiterleitung nur bei Ihren Geschäftspartnern und Kunden lächerlich.
- Private Mails: Am besten benutzen Sie für jegliche Kommunikation, die nicht im engen Sinne geschäftlich ist, eine andere rein private Mail–Adresse und fragen diese Adresse auch ausschließlich mit Ihrem privaten PC ab.
- Verschlüsselung gegen unberechtigte Kenntnisnahme: Wertvolle Unternehmensinformationen wie Geschäftsgeheimnisse, Kalkulationen, Angebote etc. also alles, was Mitbewerber oder die Öffentlichkeit nicht sehen sollen, darf nur verschlüsselt per e–Mail versandt werden. Verschlüsselungsprogramme lassen sich einfach in das Mail–Programm einbauen. Damit stellen Sie sicher, dass ausschließlich der berechtigte Empfänger Ihre Mail lesen kann – und kein Kollege und kein Unberechtigter.

  Meist bieten die Verschlüsselungsprogramme auch eine Form der digitalen Signatur an, mit deren Hilfe der Empfänger die Korrektheit der e–Mail überprüfen kann – damit ist er sicher, dass er die Mail so erhalten hat, wie Sie sie abgeschickt haben – unverändert und unmanipuliert.

  Setzen Sie ausschließlich internationalen Standards (PGP oder S/MIME) entsprechende Produkte ein.
- Datensicherung – backup: Unverzichtbar ist die regelmäßige (mind. tägliche) Sicherung aller eingegangenen und versandten e–Mails. Denn häufig genug bricht das Betriebssystem zusammen oder das e–Mail Programm stürzt ab – jedenfalls können dabei die Mailboxen so beschädigt werden, dass sie nicht mehr lesbar sind.

  Lassen Sie regelmäßig überprüfen, ob die Datensicherung korrekt abgewickelt wird – am besten dadurch, dass Sie alle gesicherten Mails auf einem anderen Computer wiederherstellen lassen und diese kontrollieren.
- Patches: Die Hersteller von Mail–Programmen bieten in Abständen Verbesserungen und insbesondere Fehlerbehebungen (sog. Patches) an; insbesondere die Patches sollten Sie unverzüglich installieren, wenn sie sicherheitsrelevante Fehler ausmerzen!
- Schulung und Sensibilisierung der Mitarbeiter: Informieren Sie Ihre Mitarbeiter über die Missbrauchsmöglichkeiten und Risiken und auch die Sicherheitsmaßnahmen. Vorbeugende Sensibilisierung und Schulung im Sicherheitsbereich macht sich in jedem Fall bezahlt.

Aufpassen, wenn ein Virus auftaucht

Plötzlich sind alle Daten oder alle Tabellen oder alle Wortdateien oder alle Grafiken oder alles zusammen gelöscht. Kunden beschweren sich über angebliche Mails – die aber keiner aus Ihrem Unternehmen versandt hat. PCs lassen sich nicht mehr starten.

Viren und Würmer sind die häufigsten Schädigungen in Unternehmen – die Schadenssummen sind deswegen ausgesprochen hoch, weil die Viren mühsam aus allen Dateien auf Computern und Datenträgern wie (Zip–)Disketten, CDs, portablen Platten sorgfältig entfernt werden müssen.

Aber Viren kommen nicht 'angeflogen', sondern werden unbemerkt per Mail oder Datenträger weitergegeben oder beim Surfen über sog. aktive Inhalte. Viren sind – im Gegensatz zu Würmern – keine eigenständigen Programme, sie benötigen daher ein Wirtsprogramm. Sie können daher auch nur in ausführbaren Programmdateien auftauchen. Einmal auf einem Computer kopieren sie sich beliebig oft in andere Dateien – und zerstören diese häufig dabei. Gegen diese Verbreitung von Viren lassen sich einfache und wirkungsvolle Sicherheitsmassnahmen ergreifen.

- Mailanhänge – attachements: E–Mails selbst enthalten daher keine Viren; vielmehr sind sie in den Anhängen (attachements) von Mails enthalten. Öffnen Sie daher nie (!) den Anhang von Mails, ohne ihn auf Viren geprüft zu haben. Das gilt für ausführbare Dateien (.exe o.ä.) genauso wie für Text–, Tabellen– und Bilddateien.

  Schalten Sie dazu auch Funktionen Ihres Mail–Programms wie das automatische Öffnen der Anhänge ab.

- Surfen im Internet: Auf vielen Webseiten sind schädigende Funktionen wie Viren, Würmer oder trojanische Pferde (Programme mit versteckten, undokumentierten Funktionen) heimlich eingebaut. Surfen Sie daher möglichst nur auf Ihnen vertrauenswürdigen Webseiten.

- Unbekannte Software und Programme: Laden Sie keinerlei Programme aus dem Internet – von Servern, denen Sie nicht voll vertrauen.

- Nutzen Sie ausschließlich Software und Programme, die Sie überprüft haben oder von anderen – möglichst Unabhängigen – überprüft wurde.

- Virensuchprogramme: Installieren Sie in jedem Fall ein sehr gutes Virensuchprogramm. Einmal installiert filtert es alle (!) Mails und auch die aus dem Internet geladene Dateien auf Viren (und Würmer) und eliminiert diese oder löscht gleich die gesamte Mail zusammen mit dem Anhang. Stellen Sie dazu das Suchprogramm so ein, dass Ihnen automatisch die neueste Fassung schnellstmöglich gesendet und sofort installiert wird. Naturgemäß können Virensuchprogramme grundsätzlich nur die Viren erkennen, deren Muster (Signatur) sie gespeichert haben. Installieren Sie die jüngste – alle bekannten sicherheitsrelevanten Fehler – korrigierende Fassung der Software. Die Kosten solcher Programme sind gering.

  Diese Suchprogramme merzen meist auch sog. Dialerprogramme aus. Dialerprogramme 'verbiegen' die zu Ihrem Internet–Provider gespeicherte Telefonnummer und leiten Ihre gesamte Kommunikation über kostenträchtige 0190–Nummern. Das kann leicht zu Kosten von mehreren 1.000 Euro pro Tag führen.

- Konfiguration: Wenn Sie das Suchprogramm auf einem Mail–Server gleich hinter Ihrer Firewall installieren, ist Ihr Unternehmen virenfrei – wenn nicht Viren auf unkontrollierten Datenträgern wie CDs, Disketten, Streamerbändern, USB–Sticks, portablen Platten etc. weitergegeben werden; diese Datenträger müssen in jedem Fall vor (!) jeder Nutzung im Unternehmen erneut überprüft werden. Ein Virensuchprogramm muss daher zusätzlich noch auf jedem PC installiert werden.

  Sie können auch auf dem Mail–Server gleich alle Anhänge ausfiltern und löschen, deren Dateiname auf VBS, SHS, EXE, COM, SCR, CHM oder BAT endet, weil Sie diese kaum im Unternehmen benötigen werden. Dies gilt auch für Dokumentennamen mit 2 oder mehr

Endungen (getrennt durch einen Punkt). In Dateien mit solchen Endungen sind Viren häufiger verpackt.

- Notfallplan: Im schlimmsten Fall kann ein Virus Ihre Daten ganz oder teilweise zerstört haben. Für diesen Fall benötigen Sie eine Sicherungskopie aller (!) Ihrer Daten, die Sie an sicherer Stelle aufbewahren. Kopieren Sie diese Daten erst dann auf Ihre Computer zurück, wenn der Virus nachgewiesen vollständig auf allen Ihren Computern gelöscht ist.

  Legen Sie im Detail fest, was außerdem unternommen werden muss, wenn trotz aller Sicherheitsmassnahmen ein Verdacht auf Virenbefall auftaucht: Alarmierung des Sicherheitsbeauftragten, Systemadministrators. Und wer löscht den Virus und gibt die befallenen Systeme wieder frei?

  Ergreifen Sie auch sofort die Initiative, wenn sich Kunden oder Zulieferer bei Ihnen als Absender eines Virus beschweren. Dann hat Ihr Virenkonzept nicht vollständig funktioniert. Informieren Sie in diesem Fall auch alle möglicherweise Betroffenen über die von Ihnen ergriffenen Maßnahmen.

- Schulung und Sensibilisierung der Mitarbeiter: Informieren Sie Ihre Mitarbeiter über die Missbrauchsmöglichkeiten und Risiken und auch die Sicherheitsmaßnahmen. Vorbeugende Sensibilisierung und Schulung im Sicherheitsbereich macht sich in jedem Fall bezahlt.

Aufpassen, wenn Daten verloren sind: Backup

Gespeicherte Daten gehen – ohne erkennbaren Grund – verloren, sind nicht mehr auffindbar, sind gelöscht, werden manchmal auch versehentlich gelöscht. Dies kann auch bei der Verarbeitung geschehen. Platten können (teilweise) nicht mehr lesbar sein. Dies gilt insbesondere bei Wasserschäden oder nach einem Feuer. Auch Viren können Ihre Daten löschen. Unverzichtbar ist daher eine vollständige Kopie aller Daten: Datensicherungskopie – Backup. Nur dann bleibt der Wiederherstellungaufwand überschaubar und Ihr Unternehmen ist binnen weniger Stunden wieder arbeitsfähig.

- Regelmäßiges Backup: Da wir nicht wissen, wann einer dieser Notfälle eintritt, muss ein regelmäßiges Backup durchgeführt werden: Mindestens täglich sollte ein Backup durchgeführt werden, zusätzlich noch während und unmittelbar nach umfangreichen oder wichtigen Arbeiten.

  Jedenfalls müssen alle Arbeiten, die nach dem letzten Backup stattgefunden haben, erneut durchgeführt werden. Legen Sie daher den Rhythmus der Datensicherung so, dass Sie möglichst wenig nacharbeiten müssen.

- Transparenz: Führen Sie das Backup für alle (!) Ihre Computer durch – unabhängig von dem aktuellen Bedarf. Lassen Sie das Backup grundsätzlich programmgesteuert durchführen (z.B. nachts) und belasten Sie mit dieser Aufgabe nicht jeden oder auch nur einen Mitarbeiter.

- Vollständigkeit: Lassen Sie alle Daten sichern und denken Sie nicht erst darüber nach, welche wichtig oder weniger wichtig sind und vielleicht nicht unbedingt gesichert werden müssen.

  Lassen Sie gleichermaßen alle installierten Programme sichern – sie sparen sich bei einem Ausfall die erneute Konfiguration.

  Notieren Sie die Typenbezeichnungen aller eingesetzten Hardware und Software und bewahren Sie diese Listen so sicher wie die Backups auf. Nach einem Brand oder einem anderen Notfall brauchen Sie neben den Daten nämlich die Software und die Hardware – und zwar genau in der Konfiguration, wie Sie eingesetzt war. Sie erhalten gewiss schnell Ersatz für die ausgefallene Hardware, wenn Sie nur wissen, was Sie brauchen.

- Kontrolle: Überprüfen Sie nach jedem Backup, ob Ihre Daten auch korrekt gesichert wurden. Häufig genug wurden die Parameter falsch eingestellt und nichts (!) gespeichert.

  Lassen Sie in unregelmäßigen Abständen Ihre Daten von der Datensicherungskopie zurückspielen auf einen Computer, um das Verfahren aufkorrekten Ablauf zu überprüfen. Benutzen Sie dazu einen Testcomputer und keinesfalls einen Produktionscomputer, sonst zerstören Sie sich womöglich selbst die Originaldaten.

- Speichermedien: Das preiswerteste Medium sind Bänder oder Streamerbänder – sie sind aber auch langsam. Bei geringen Mengen können Sie Ihre Daten aber auch auf CDs oder Disketten sichern –. Das teuerste Medium sind portable Magnetplatten – sie lassen sich am schnellsten beschreiben und wieder lesen und auf ausgewählte Daten kann direkt zugegriffen werden – dagegen muss ein Band erst lange durchlaufen bis hin zur gewünschten Datei.

  Da Backups meist nachts durchgeführt werden, spielt die Schreibgeschwindigkeit eine geringe Rolle. Da die Datenträger nur im (seltenen) Notfall wieder eingespielt werden müssen, ist auch die Lesegeschwindigkeit nicht so sehr wichtig.

  Müssen Daten nach einem Verlust sehr kurzfristig wieder zur Verfügung stehen, werden u.a. hot–stand–by Computer installiert, auf denen alle Daten gespiegelt vorhanden sind. Diese Computer können im Notfall sofort alle Aufgaben übernehmen und nahtlos weiterarbeiten.

  Ein Mittelweg ist das Spiegeln von Daten auf einen anderen, entfernten Computer. Der Vorteil dieser beiden Lösungen ist die Aktualität der gesicherten Daten – ohne jegliches Nacharbeiten.

- Generationenprinzip: Schreiben Sie das Backup nicht immer wieder auf dasselbe Speichermedium. Benutzen Sie vielmehr mehrere Generationen von Datensicherungskopien. Dies für den Fall, dass eine Kopie aus technischen Gründen verloren geht, die Daten nicht lesbar sind, der Datenträger punktuell defekt ist o.ä.
- Aufbewahrung: Bewahren Sie die jeweils jüngste Generation im Unternehmen auf – allerdings in einem Datenträgerarchiv und nicht in Räumen mit Computern oder brennbaren Materialien wie Papier. Bewahren Sie das Backup – möglichst in einem anderen Gebäude – in einem brand– und wassergeschützten Stahlschrank, Panzerschrank oder Tresor auf.

  Die jeweils zweite Generation sollte außerhalb des Unternehmens gelagert werden – z.B. in einem Stahlschrank eines befreundeten Unternehmens oder einer Bank.

  Die jeweils dritte Generation sollte stark geschützt in einem Felsenkeller untergebracht werden – weit entfernt vom Unternehmen.

Aufpassen, wenn Ihre Software veraltet: Patches

Software wie Betriebssysteme, Datenbanksysteme und Anwendungssoftware enthalten viele – auch viele sicherheitsrelevante Fehler. Dies liegt an ihrer Komplexität, ihrer Entwicklungsqualität und an der eingesetzten Programmiertechnik auch der größten Softwareunternehmen. Dabei sind ordentliche Programmiertechniken und auch Testverfahren weltweit bekannt – werden aber nur deswegen nicht oder zu selten eingesetzt, weil ihr Einsatz etwas kostet. Die Hersteller können sich dies erlauben, weil die Rechtsprechung eine (dringend notwendige) Produkthaftung für Software bisher nicht vorsieht. Dies dürfte sich in den nächsten Jahren ändern. Bis dahin, müssen wir Anwender mit den Unzulänglichkeiten, Mängeln und Fehlern von Software leben.

Eine ganze Reihe dieser Fehler betrifft die Sicherheit der Programme. Durch diese sicherheitsrelevanten Fehler können wichtige Unternehmensdaten unberechtigten Dritten – unberechtigten Mitarbeitern und auch Außenstehenden – zur Kenntnis kommen und auch von diesen manipuliert werden. Die Hersteller veröffentlichen daher in unregelmäßigen Abständen Fehlerkorrekturen – sog. Patches

- Fehlerkorrekturen und Patches: Sicherheitsrelevante Schwachstellen werden von den Softwareherstellern meist erst zusammen mit der zugehörigen Fehlerkorrektur veröffentlicht. Das hat für den Anwender zwei Folgen:
  - Angreifer haben ggf. längst die Schwachstelle erkannt oder sind von Kriminellen auf diese Schwachstelle hingewiesen worden und nutzen sie zu einem Angriff aus. Nur Ihnen ist die Schwachstelle nicht bekannt und Sie können sich daher auch nicht gegen diese Angriffe schützen!
  - Sowie die Fehlerkorrektur zusammen mit der zugrundeliegenden Schwachstelle veröffentlicht ist, weiß die ganze Welt von der Schwachstelle. Dementsprechend erreicht die Zahl der Angriffe auf die jetzt bekannte sicherheitsrelevante Schwachstelle jeweils am darauffolgenden Wochenende ihren Höhepunkt. Angreifer hoffen nämlich zu recht, dass die Anwender die Fehlerkorrektur (noch) nicht eingebaut haben. Erfahrungsgemäß lassen sich Anwender damit häufig 1 Jahr oder länger Zeit!

  Sie haben also nur bis zum jeweils nächsten Wochenende Zeit, um einen Patch einzufahren.
- Prüfung von Patches: Vor einem Einsatz müssen die Patches von Ihnen unter mehreren Gesichtspunkten sorgfältig überprüft werden:
  - Ist das Produkt in Ihrem Unternehmen vorhanden und auch im Einsatz?
  - Sicherheitsrelevanz für Ihre Anwendung: Ist die Anwendung und sind die damit verarbeiteten Daten wirklich wichtig für Ihr Unternehmen?
  - Haben Sie den Patch von einer vertrauenswürdigen Webpage geladen – oder sieht die Seite nur so aus, ist aber tatsächlich manipuliert? Hier hilft die Überprüfung von Zertifikaten, durch die sich der Hersteller ausweist.
  - Funktionsfähigkeit des Produkts nach der Fehlerkorrektur: Oft genug hat zwar der Patch seine Fehlerkorrekturfunktion erfüllt – der Patch weist aber nicht–dokumentierte Nebenfunktionen auf, die Ihren Betrieb erheblich stören können. Im Einzelfall haben Patches den Durchsatz des Betriebssystems auf 5% reduziert!
  - Verträglichkeit mit Ihrer übrigen Software – denn die muss ja schließlich noch weiterhin funktionieren.

  Wollen Sie nicht Vorreiter und Tester der Patches für den Hersteller (und alle seine Kunden) sein, empfiehlt sich ein Abwarten, bis andere Anwender den Patch überprüft haben und ob der jeweilige Test überhaupt diesen Grundanforderungen entspricht!
- Patches im Update: Im Einzelfall sind sicherheitsrelevante Korrekturen auch in einer neuen Fassung (Update) des Programms enthalten. Das hat zur Folge, dass Sie das Update erwerben müssen.
- Aktualität: Allerdings richten Sie die meisten Angriffe gegen vor längerer Zeit (ein halbes

bis zu einem Jahr!) veröffentlichte sicherheitsrelevante Schwachstellen, die durch einen ebenfalls längst veröffentlichten Patch hätten behoben sein müssen. Die o.g. Überprüfungen müssen von Ihnen also sorgfältig und zeitnah durchgeführt werden, um über den Einsatz eines Patches in Ihrem Unternehmen entscheiden zu können.

- Zahl der Patches: Eine weitere Schwierigkeit ergibt sich aus der großen Zahl der sicherheitsrelevanten Schwachstellen und der Anzahl der veröffentlichten zugehörigen Patches: Pro Tag wurden im letzten Jahr etwa 2.000 sicherheitsrelevante Schwachstellen mit zugehörigen Patches veröffentlicht – das entspricht mehr als 8 pro Arbeitstag.

  Daher müssen Sie sorgfältig überprüfen lassen, welche Patches für Ihr Unternehmen wichtig sind und welche verzichtbar.

Die – unter Sicherheitsaspekten – jeweils jüngste Version der Software sollten Sie unbedingt bei allen Computern sicherstellen, die am Internet, Extranet, Intranet, LAN angeschlossen sind – und zwar für Betriebssysteme, Datenbanksysteme, Mail–Programme, Webserver und Browser sowie für jegliche Sicherheitssoftware wie Virensuchprogramme, Auditing und Intrusion Detection und Prevention, Firewalls etc.

Aufpassen, wenn Ihr PC kontrolliert werden muss

Gegen Hacker, Cracker, Passwort–Knacker schotten sich viele Unternehmen bereits erfolgreich mit Firewalls und Virensoftware ab. Den Sabotageversuchen ihrer eigenen Mitarbeiter aber sind sie schutzlos ausgeliefert.

Bei der Verteidigung ihrer Computersicherheit sind die meisten Firmen nur auf einen Angriff von außen fixiert - und verkennen dabei, dass die größte Gefahr oftmals in den eigenen Reihen lauert. Denn gezielte Angriffe fahren Kids der Kategorie Hacker, Cracker, Passwort–Knacker nur sehr selten. Sie wissen dafür viel zu wenig über das Unternehmen, dessen Sicherheitsmaßnahmen, die Netzstruktur.

Bei schadenträchtigen Spionagefällen und Sabotageakten stellt sich deshalb in fast allen Fällen heraus, dass sie von Innentätern begangen wurden. Oder von Außenstehenden, die von den eigenen Leuten gezielt über die Sicherheitsmaßnahmen informiert wurden - gelegentlich auch von Mitarbeitern, die gutgläubig oder fahrlässig derart wichtige Informationen weitergeben.

So schützen sich Unternehmen gegen Innentäter:

- Restriktive Zugriffskontrolle: Jeder Mitarbeiter darf nur auf die Daten zugreifen, die er für seine Arbeit braucht. Wichtig: Diese Zugriffsrechte regelmäßig auf Korrektheit und Notwendigkeit überprüfen.
- Alle Passwörter in unregelmäßigen Abständen ändern. Dabei auch die Sicherheitsqualität der benutzten Passwörter kontrollieren: Sie sollten mindestens 6 Zeichen haben, möglichst 8, und nicht nur aus Alphazeichen bestehen, sondern auch mit Ziffern und Sonderzeichen bestückt sein. Weitsichtige Firmen überprüfen zudem, ob die Passwörter überhaupt gewechselt wurden. Denn manche Mitarbeiter wechseln gleich zweimal: Einmal zu einem schwierig zu merkenden Passwort und dann gleich wieder zurück zum alten.
- Um mögliche Fehlzugriffe oder gar Angriffe erkennen zu können, sollten Firmen die Protokolle von Betriebssystem, Router, Firewall, Anwendungssoftware etc. ständig auswerten. Tipp für Firmenchefs: sich eine Zusammenfassung der Auswertung regelmäßig vortragen lassen und die Anweisung geben, dass sie bei Missbrauch oder auch nur wiederholten Fehlzugriffen auf wichtige Dateien sofort zu informieren sind.
- Jegliche private Nutzung des Internets strikt unterbinden. Abgesehen vom zeitlichen Aufwand fürs Surfen entstehen Kosten für die Nutzung des Internets. Wenn Firmenchefs glauben, sie könnten dies in der Belegschaft nicht durchsetzen, sollten sie durch ihren Computerspezialisten jene drei Web-Adressen feststellen lassen, die in ihrem Unternehmen am häufigsten benutzt wurden. Hier haben schon manche Unternehmer Überraschungen erlebt.
- Alle Computer in unregelmäßigen Abständen auf Spiele(!) überprüfen, Bilder und was sonst noch übers Internet heruntergeladen werden kann - sowie auf eventuell eingespielte Viren.
- Jeden strafrechtlichen Fall (Kinderpornografie etc.) sofort zur Anzeige bringen. Alle Mitarbeiter über diese Konsequenzen von vornherein informieren und ihnen den Imageschaden vor Augen führen, den das Unternehmen erleidet, wenn es wegen kriminellen Verhaltens auch nur eines einzigen Mitarbeiters in die Schlagzeilen gerät: Aufträge könnten storniert werden, Arbeitsplätze geraten in Gefahr.

\- - -