Digitale Forensik

Dipl-Ing. Thomas Käfer

3. Ausgabe

Datensicherung-Datensicherheit-Datenschutz
Security-Update 2013

www.KaeferLive.de

DigiFor Inside 3. Ausgabe

Datensicherung - Datensicherheit - Datenschutz – Security-Update 2013.

Impressum

Herausgeber: KäferLive - Dipl.-Ing. Thomas Käfer
Elchenrather Weide 20
52146 Würselen
Tel. 02405/47949-0

Autor: Dipl.-Ing. Thomas Käfer
Öffentlich bestellter und vereidigter Sachverständiger
für Systeme und Anwendungen der Informationsverarbeitung

Website: http://www.KaeferLive.de
E-Mail: service@KaeferLive.de

Bildnachweis: Quelle Fotolia.com bzw. eigene Aufnahmen/Grafiken

Bezug und weitere Informationen und Artikel siehe:
http://www.KaeferLive.de/

ISBN-Nr.: 978-3-944632-12-4 (Apple iBook®-Format)
978-3-944632-07-0 (ePub)
978-3-944632-08-7 (PDF)

Erscheinungsdatum Mai 2013


KäferLive Portalsystem
www.kaeferlive.de

Inhalt

DigiFor Inside

Was ist DigiFor Inside? DigiFor ist die Kurzform für den Begriff „Digitale Forensik“, einem Spezialgebiet der IT, welches sich mit der Analyse und Aufdeckung von Sicherheitsvorfällen (sogenannten Incidents) und missbräuchlicher Nutzung von Computern im Rahmen von Straftaten und zivilrechtlichen Auseinandersetzungen beschäftigt. DigiFor Inside ist eine neue Reihe von Fachaufsätzen und Veröffentlichungen, publiziert auf dem Portal KäferLive (http://www.KaeferLive.de/digifor-inside), bei denen der Autor Thomas Käfer aus dem IT-Nähkästchen plaudert und Angriffskonzepte und Maßnahmen zu deren Erkennung bzw. Abwehr offen legt.

Mit diesem Artikel liegt nun bereits die 3. Ausgabe der DigiFor-Inside-Reihe vor (siehe http://www.KaeferLive.de/digifor-inside).

Datensicherung - Datensicherheit - Datenschutz

Der Artikel Datensicherung - Datensicherheit - Datenschutz aus der Reihe DigiFor Inside beschäftigt sich im Schwerpunkt mit den verschiedenen Aspekten der Absicherung von elektronisch gespeicherten und übertragenen Daten.

Der Duden liefert zum Begriff „Sicherheit“ die folgende Definition: *Zustand des Unbedrohtseins, der sich objektiv im Vorhandensein von Schutzeinrichtungen bzw. im Fehlen von Gefahrenquellen darstellt und subjektiv als Gewissheit von Individuen oder sozialen Gebilden über die Zuverlässigkeit von Sicherungs- und Schutzeinrichtungen empfunden wird*.

Damit sich dieses Gefühl zu Recht beim Nutzer bzw. Inhaber der Daten einstellt, gilt es, einige technologische, rechtliche und verfahrenstechnische Grundsätze zu kennen, zu beachten und anzuwenden.

Die nachfolgende Abhandlung erklärt daher aus verschiedenen Blickwinkeln, wie der Schutz vor missbräuchlicher Nutzung initial hergestellt und dauerhaft sichergestellt werden kann, wie konkrete Bedrohungsszenarien aussehen können und wie man sich gegen diese schützen kann.

Begriffsbestimmungen

Für das weitere Verständnis ist es ungemein wichtig, die Begriffe „Datensicherung“, „Datensicherheit“ und „Datenschutz“ korrekt anzuwenden und zu unterscheiden:

Datensicherung

Mit dem Begriff „Datensicherung“ ist der Schutz der Daten vor Verlust oder Zerstörung durch Rückgriff auf gesicherte Versionen gemeint.

Datensicherheit

Unter „Datensicherheit“ versteht man den Schutz der Daten vor missbräuchlicher Nutzung oder Einsichtnahme durch fremde Dritte (Angreifer von außen).

Datenschutz

Mit „Datenschutz“ bezeichnet man den Schutz von personenbezogenen Daten vor missbräuchlicher Nutzung durch die erfassenden oder weiter verarbeitenden Benutzer.

Zielgruppe

Dieser Artikel richtet sich gleichermaßen an EDV-Anwender und -Entscheider als auch an IT-Sicherheitsbeauftragte und Administratoren und bietet in der täglichen Praxis anwendbare Sicherheitshinweise und empfohlene Richtlinien, um Schwachstellen in Systemen oder bei der Handhabung zu schließen bzw. erst gar nicht entstehen zu lassen. Der interessierte Leser und Computer-Anwender findet in den vertiefenden Kapiteln fachlich fundierte Informationen u.a. zu den Themen Datensicherheit, Backup, Angriffsszenarien, Computer Forensik und Datenschutz.

Abgrenzung

Die im vorliegenden Dokument beschriebenen Mechanismen und Konzepte können natürlich auch von der „dunklen Seite der IT“ als Anleitung verstanden oder benutzt werden, wie man einen Angriff auf fremde Daten konzipiert. Dies ist nicht die Intention des Autors bzw. des Fachaufsatzes und mutmaßlich für erfahrene Hacker überflüssig. Jeder, der dieses oder vergleichbares Wissen dazu nutzt, Schad-Code in fremde Systeme einzuschleusen und sich unbefugt Daten Dritter zu bemächtigen, sollte sich bewusst machen, dass jede konkrete Aktion zum Überwinden von fremden Schutzmaßnahmen, ein Eindringen in IT-Systeme anderer oder das Abschöpfen von persönlichen Daten bereits eine strafbare Handlung darstellt. Datendiebstahl oder gar das Ausnutzen der gestohlenen Daten, um sich zu bereichern, ist kein Kavaliersdelikt und auch kein Sport!

Der Autor

Der Autor - Dipl.-Ing. Thomas Käfer - beschäftigt sich seit mehr als zwei Jahrzehnten professionell mit dem Werkzeug „Computer“ und seit geraumer Zeit mit dem Aspekt der IT-Sicherheit und der Digitalen Forensik. Seit dem Wintersemester 2012 bildet er sich nebenberuflich im Rahmen des Masterstudiengangs Digitale Forensik an der Hochschule Albstadt-Sigmaringen aktiv und intensiv weiter. Im Studium und bei der täglichen Arbeit als öffentlich bestellter Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung bzw. IT-Consultant wird er regelmäßig mit unterschiedlichen Aspekten der missbräuchlichen Nutzung der EDV konfrontiert. Kernaufgabe als Sachverständiger bzw. Forensiker ist die Aufdeckung von Delikten, bei dem der Computer zur Waffe bzw. Ziel eines Angriffes geworden ist.

Datensicherung: Der Retter in der Not

Beginnen wir mit dem möglicherweise wichtigsten Aspekt im Themenkomplex Schutz und Sicherheit von Daten, der Datensicherung oder neudeutsch dem Backup. Warum? EDV funktioniert erst einmal ohne Datensicherung, Netz und doppelten Boden. Aber es ist nur eine Frage der Zeit, bis man zum ersten Mal auf ein Backup zurückgreifen muss. Hat man nie eine Datensicherung eingerichtet, dann tritt bei einem sicherheitskritischen Vorfall der Worst-Case ein und man kann – frei nach Peter Fox – nur noch „Mach neu!“ empfehlen.

Datensicherung oder Backup ist Chefsache und gehört damit zur wichtigsten Anwenderpflicht beim Einsatz der EDV. Die Gründe für einen Datenverlust sind vielfältig: Technische Ausfälle, Anwenderfehler, Datenmanipulationen oder sicherheitsrelevante Vorkommnisse, um nur die wichtigsten zu nennen.

Allein schon bei der Betrachtung einer Festplatte (oder jedem anderen Speichermedium) stellt sich nicht die Frage, **ob** eine Festplatte ausfällt, sondern **wann**! Ein durchdachtes Datensicherungskonzept ist somit Retter in der Not und gehört z.B. im Forderungskatalog von Kreditinstituten (Rating[1]) oder im Bereich eines qualitativ hochwertigen und prozessorientierten Denkens an die oberste Stelle.

[1] Einfluss über so genannte „weiche“ Ratingfaktoren auf Einschätzung der Kreditinstitute bei der Vergabe von Krediten (Konditionen und Kreditlinien)

Zielsetzungen bei der Datensicherung

- Sicherung der aktuellen Version
    - Schneller Zugriff bei Systemausfall (Minimierung der Ausfallzeit)
    - Primär Absicherung gegen Datenverlust durch fehlerhafte Hardware (speziell Festplatte)
- Sicherung der Daten in verschiedenen Versionen (Archivierung)
    - Zugriff bei Datenverlust auf aktuelle oder ältere Versionen (grundsätzliche Möglichkeit zum Rückgriff auf gesicherte Daten)
    - Primär Absicherung gegen Datenverlust durch
        - Benutzerfehler
        - fehlerhafte Systeme (Hard- und/oder Software)
        - Datenmanipulationen

Datenspiegelung

Ein Schritt zu mehr Datensicherheit ist die Verwendung von hochwertigen, für den Dauereinsatz konzipierten Festplatten. Im Serverbereich haben sich hier seit Jahren sogenannte SCSI-Festplatten bewährt, die im Vergleich zu den in Desktop-PCs verwendeten (billigen) Festplatten nach IDE/ATA- bzw. SATA-Standard neben höheren Übertragungsgeschwindigkeiten und niedrigeren Zugriffszeiten auch entsprechend eine hohe Lebensdauer besitzen.

Besonders zu beachten ist hierbei die sogenannte MTBF-Zeit (Mean Time Between Failures), die die statistisch ermittelte durchschnittliche Zeit zwischen dem Auftreten zweier Fehler (also bis zum nächsten, nicht aber zwangsläufig bis zum ersten Fehler) beziffert. Ein hoher MTBF-Wert (der schon einmal deutlich über der voraussichtlichen Einsatzzeit des Systems liegen sollte) ist ein Indikator (kein Garant) dafür, dass die Festplatte die vorgesehene Betriebszeit ohne Fehler / Ausfall übersteht.

Ein weiterer wesentlicher Unterschied zwischen SCSI-(Server-) Festplatten und SATA-(Arbeitsplatz-) Harddisk liegt darin, dass die SCSI-Versionen für einen Dauerbetrieb ausgelegt sind, nicht aber für ein häufiges Neustarten (Kaltstarts, teilweise nur im Bereich von wenigen Hundert Neustarts). Letzteres ist die Domäne der Workstation-Harddisks, die man deutlich öfter anfahren kann, dafür aber nicht dauerhaft in Betrieb haben sollte.

Aber auch das beste Produkt kann ausfallen und daher gehört in einen guten Server (oder eine wichtige Workstation) mindestens eine zweite baugleiche Festplatte zur Daten-Spiegelung (RAID 1). Dabei sorgt ein spezieller Controller oder das Betriebssystem dafür, dass die Daten, die von einem Benutzer auf der Hauptfestplatte gespeichert werden, mit minimaler Zeitverzögerung auch auf die zweite Platte geschrieben werden. Hierdurch erhält man eine ständig aktualisierte 1:1 Kopie der Primärplatte, mit der man bei Ausfall der Hauptplatte das System wieder exakt mit den letzten gespeicherten Daten hochfahren und somit weiterarbeiten kann. Somit kann ein Techniker in Ruhe eine neue Festplatte einbauen und die Spiegelung wieder aktivieren: Ausfallzeit i.d.R. wenige Minuten. Ein solches Verfahren lässt sich recht preiswert durch zwei baugleiche (bzw. gleich große) SCSI-Festplatten (Parallel-SCSI) realisieren.

Die Krönung dieser Technik ist ein sogenanntes RAID Level 5 (bzw. Level 6 oder Level 10) System, bei dem mehrere Festplatten (mindestens drei) durch aufwendige Verfahren so mit den Daten bespielt werden, dass irgendeine dieser Platten ausfallen kann und im Fall einer mitlaufenden Reserveplatte (Hot-Spare) das RAID sogar ohne direkten Technikereinsatz mit entsprechender Datensicherheit (Redundanz) weiterläuft.

Mittlerweile haben sich neben den SATA-Festplatten (Serial ATA) auch sogenannte SAS-Harddisks etabliert (Serial Attached SCSI). Der SATA- bzw. SAS-Standard hat den Vorteil, dass für beide Controllertypen, die gleichen Anschlüsse benutzt werden und sich somit einfachere und flexibel nutzbare Festplattensubsysteme aufbauen lassen. Die SAS- ist der SATA-Version aus Gründen der Performance und Lebensdauer vorzuziehen, jedoch auch deutlich teurer als das entsprechende SATA-Gerät.

Ein Kompromiss kann darin bestehen, ein RAID System Level 6 oder höher aus Kostengründen mit SATA-Festplatten aufzubauen, den Ausfall einer Platte billigend in Kauf zu nehmen und durch Bevorratung passender Ersatzplatten zu kompensieren.

In Anbetracht heutiger Festplattengrößen gilt es jedoch, auf ein weiteres Problem zu achten. Die Hersteller von Festplatten geben für die Harddisks die Wahrscheinlichkeit für einen nicht korrigierbaren Lesefehler an (URE bzw. Unrecoverable Read Error). Dieser Wert liegt typischerweise bei 10^{-14} bis 10^{-16}. Man beachte den negativen Exponent: Ein höherer Absolutwert des Exponents bedeutet eine geringere Wahrscheinlichkeit für einen Fehler – 10^{-16} ist also besser als 10^{-14}!

Ein Wert von 10^{-14} bedeutet, dass auf 10^{14} gelesene Bits ein Fehler kommt.

Diese 10^{14} Bit entsprechen etwa 12 TB. Besteht ein Array nun also z.B. aus 8 je 2 TB großen Festplatten, so ergibt sich nur noch eine statistische Wahrscheinlichkeit für ein erfolgreiches Rebuild von 1:3, d.h. 2 von 3 Rebuild-Versuchen schlagen wahrscheinlich fehl. Damit ist ein solches RAID-System bei Ausfall einer Festplatte und einem nachfolgenden Rebuild praktisch wertlos!

Eine Abhilfe liegt darin, entweder höherwertige Platten (RAID-Zertifizierung bzw. URE-Werte im Bereich 10^{-15} bzw. 10^{-16} oder kombinierte RAID-Levels (10 oder 50) zu nutzen.

Auch wenn die URE-Werte rein statistischer Natur sind und in der Praxis durchaus besser sein können, sollte man diesen Rat ernst nehmen, denn nach Murphy geht im Zweifelsfall alles schief, was schief gehen kann (und die URE-Werte verschlechtern sich durch Alterung und Verschleiß!).

Offline Backup mit Medieneinsatz

Dies alles ist kein Schutz gegen bewusst oder unbewusst durch die Benutzer oder durch Fehlfunktion der Software (incl. Viren) initiierte Datenmanipulationen und -verluste. Hier greift nur ein sogenanntes Offline-Backup: eine Datensicherung, die manuell oder automatisiert gestartet Kopien der Daten auf externe und - wichtig - verschiedene Medien anfertigt. Hier haben sich Bandlaufwerke z.B. auf DAT, DLT oder LTO-Basis (o.ä.) bewährt, die in Verbindung mit einer Backup-Software nächtlich und vollautomatisch Datensicherungen auf Tapes (oder analog andere Medienformen) anfertigen. Der Benutzer (Administrator) braucht dann morgens nur das Band zu wechseln und einen Blick auf das Protokoll zu werfen, um Erfolg oder Misserfolg der Datensicherung zu erkennen. Letzteres ist enorm wichtig, da es nicht selten Fälle aus der Praxis zu berichten gibt, in denen Anwender brav täglich das Band gewechselt haben, der Backup-Prozess aber bereits seit zwei Jahren nicht mehr erfolgreich gelaufen ist.

Ein erfahrungsgemäß gutes Konzept für die Datensicherung ist das sogenannte „Großvater-Vater-Sohn-Prinzip“[2]. Hierbei bietet es sich an, an jedem Wochentag nächtlich automatisiert eine Komplettsicherung des ganzen Servers oder zumindest des Datenbereiches anzufertigen. Montags benutzt man das „Montags-Band“ (oder analog die „Montags-CD“), dienstags das „Dienstags-Band“ usw.. Nur der Freitag (analog natürlich auch ein beliebiger anderer Wochentag) wird besonders behandelt. Am ersten Freitag im Monat legt man das Monats-Band des jeweiligen Monats ein. Am zweiten Freitag im Monat das Band „Woche 2“, am dritten Freitag „Woche 3“ bis max. zum Wochenband Nr.5. Auf diese Weise ist man in der Lage, die letzten 5 Tage tagesaktuell, die letzten 5 Wochen mit dem Stand des jeweiligen Freitags und die letzten 12 Monate mit dem Stand vom ersten Freitag im Monat wiederherzustellen. Das entspricht den typischen Zugriffen auf ein Backup, da entweder sehr aktuelle Backups benötigt werden (z.B. beim Totalausfall oder dem sofortigen Bemerken eines Fehlers) oder längerfristig zurückliegende Versionsstände gefordert sind (z.B. weil nach einer „Aufräumaktion“ erst Monate später der Verlust einer doch benötigten Datei bemerkt wird).

Durch ein Rotieren der Medien untereinander (Austausch der Tages- oder Wochenbänder gegen die Verwendung als Monatsbänder) erreicht man eine Optimierung der Haltbarkeit bzw. Reduzierung des Verschleißes.

[2] Das hier vorgestellte Konzept ist eine Abwandlung der klassischen Verfahrensweise; Das Verfahren ist unabhängig vom verwendete Backup-System (Band, CD, DVD usw.).

Eigentlich unnötig zu erwähnen, jedoch trotzdem immer wieder zu beobachten: Die Medien der Datensicherung sollen nicht (alle) in der Nähe des Servers aufbewahrt werden. Am besten ist es, wenn zumindest immer einige Bänder aus dem Gebäude heraus an einen sicheren Ort verbracht werden, um die Datensicherung bei Brand, Wasserschaden, Diebstahl oder Vandalismus nicht zusammen mit dem Server zu verlieren (hierbei bitte den Datenschutz entsprechend der später behandelten Kapiteln beachten!).

Einlegereihenfolge der Bänder:

1. Woche des Monats:	Montag:	Montagsband
	Dienstag:	Dienstagsband
	Mittwoch:	Mittwochsband
	Donnerstag:	Donnerstagsband:
	Freitag:	**Monatsband des aktuellen Monats**
2. Woche des Monats:	Montag:	Montagsband
	Dienstag:	Dienstagsband
	Mittwoch:	Mittwochsband
	Donnerstag:	Donnerstagsband:
	Freitag:	**Wochenband 2. Woche**
3. Woche des Monats:	Montag:	Montagsband
	Dienstag:	Dienstagsband
	Mittwoch:	Mittwochsband
	Donnerstag:	Donnerstagsband:
	Freitag:	**Wochenband 3. Woche**
4. Woche des Monats:	Montag:	Montagsband
	Dienstag:	Dienstagsband
	Mittwoch:	Mittwochsband
	Donnerstag:	Donnerstagsband:
	Freitag:	**Wochenband 4. Woche**
Ggf. 5. Woche des Monats:	Montag:	Montagsband
	Dienstag:	Dienstagsband
	Mittwoch:	Mittwochsband
	Donnerstag:	Donnerstagsband:
	Freitag:	**Wochenband 5. Woche**

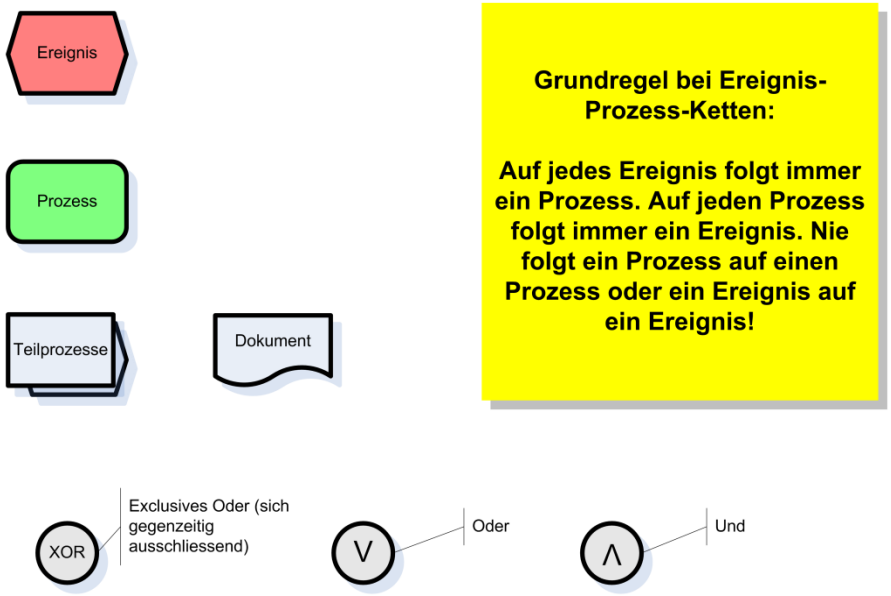
Fällt ein Freitag auf einen Feiertag bzw. ist das Wechseln des Bandes temporär nicht möglich, so kann ein Wochen- oder Monatsband ausnahmsweise natürlich auch an einem anderen Werktag beschrieben werden. Das Anfertigen und Archivieren von Wochen- und Monatsbändern hat Vorrang vor Tagesbändern! Kompliziertere Abwandlungen des Prinzips fertigen nicht immer Komplettbackups an, sondern überbrücken Zwischenphasen mit sogenannten Zuwachs- oder Inkrementalsicherungen. Damit ein solches Backup nachher den vollständigen Stand widerspiegelt, ist jedoch eine erhöhte Disziplin hinsichtlich der Bandverwendung und Auftragsdurchführung nötig. Eine sehr schlechte, aber dennoch immer wieder praktizierte Datensicherung besteht aus der wechselseitigen Verwendung von nur wenigen, meist 2 oder 3 Bändern oder Medien.

Hier wird die Datensicherung zu schnell wieder mit aktualisierten Versionen überschrieben, sodass keine älteren Versionen mehr zur Rücksicherung bereitstehen.

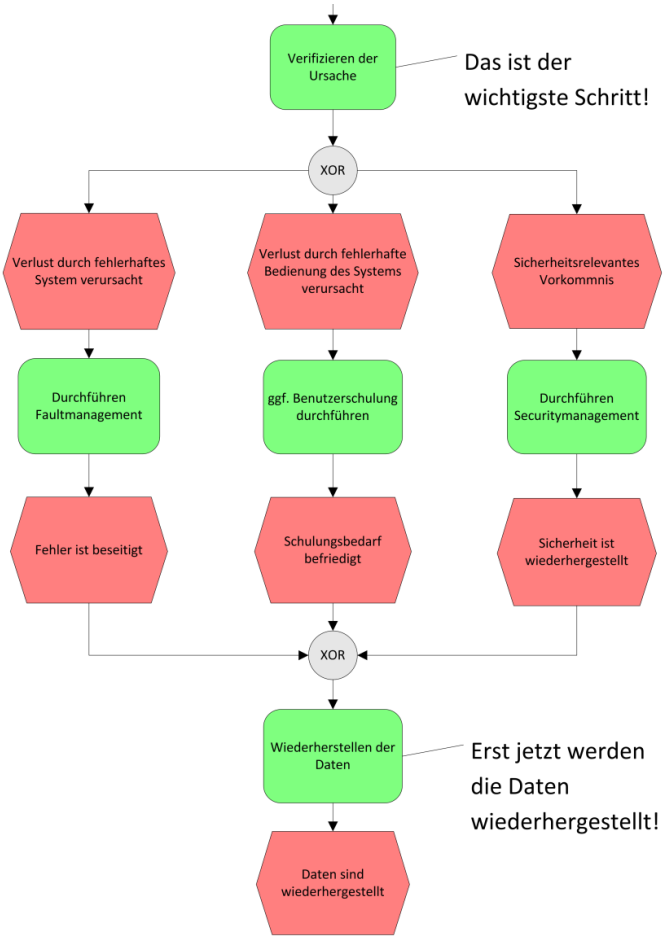
Wiederherstellung

Im Fehlerfall stellt man die Daten übrigens sinnvollerweise nicht einfach wieder her, sondern ermittelt zuerst (!) die Ursache für den Datenverlust (auch wenn es mal wieder schnell gehen muss). Denn ansonsten wiederholt sich der Fehler vielleicht sofort oder Indikatoren für ein sicherheitskritisches Problem oder einen drohenden Totalausfall der Hardware bleiben unentdeckt.

Sehr hilfreich ist z.B. das im Folgenden dargestellte Verfahren aus dem Referenzprozess für System-Administratoren (IT-Spezialisten-Zertifizierung nach ISO 17024):




Datensicherungssystem im Einsatz
Datenverlust aufgetreten
Λ
V
Störungsmeldung
Entgegennehmen der Meldung einer Datenwiederherstellung
Selbstständiges Erkennen einer Datenwiderherstellung
Anforderung entgegen genommen
Anforderung selbstständig erkannt
V
Identifizieren des Datenverlusts
XOR
Daten sind verloren
Daten sind zerstört
Daten wurden verändert
XOR
Verifizieren der Ursache
Das ist der wichtigste Schritt!



Wenn Sie weitere Informationen zur ISO 17024 Personenzertifizierung und den Referenzprozessen für die IT-Spezialisten wissen möchten, kontaktieren Sie einfach den Autor: Thomas Käfer hat in Zusammenarbeit mit der IHK Aachen ein umfangreiches Schulungs- und Zertifizierungsprogramm für die IT-Spezialisten ausgearbeitet und bereits rund 100 IT-Administratoren entsprechend geschult bzw. bei der Weiterqualifizierung begleitet.

(Info https://www.kaeferlive.de/web/sachverstaendiger/apo-coaching)

Fast Facts

- Es ist nicht die Frage, **OB** eine Festplatte ausfällt, sondern **WANN**!
- RAID-Systeme / Spiegelungen ersetzen kein klassisches Backup
- Technische Umsetzung der Datensicherung unter Verwendung von auslagerungsfähigen Medien:
    - mit CD-RW (wieder beschreibbare CDs)
    - mit DVD-RW (wieder beschreibbare DVDs)
    - mit Bändern (ADR, DAT, DLT, LTO usw.)
    - Arbeiten Sie mit so vielen verschiedenen Medien wie möglich. Nicht immer nur 2 oder 3 Medien wieder verwenden.
    - Lagern Sie die Medien aus. Nicht alle Medien unmittelbar neben dem Server lagern!

Daten – das Kapital des Unternehmens

Neben Euro und Dollar gibt es eine weitere Währung: Daten. Nutzer bezahlen Leistungen (im Internet) mit ihren Daten, Adressen und sogenannte Leads werden mit echtem Geld bezahlt und Daten sind i.d.R. die Basis jedes echten Geschäftsvorfalls.

Der kalkulatorische Wert verlorener Nutzdaten (ohne aktuelle Datensicherung) kann durchaus mit einem Wert von 500,- € pro MB angesetzt werden (Überlieferung aus der Versicherungsbranche).

Eine 50 MB Datenbank (Nutzdaten) hätte demnach einen Wert von 25.000,- €. Man kann den Wert von Daten (oder einer funktionsfähigen EDV-Anlage) auch danach beziffern, was es kostet, wenn man eine Stunde, einen Tag oder eine Woche nicht mehr handlungsfähig ist, Aufträge verloren gehen oder die Produktion still steht. Rechnen Sie selbst nach. Sie werden erstaunt sein, wie wichtig die EDV für Sie ist und was es Sie kostet, wenn sie nicht funktioniert!

- Datensicherung ist Chefsache
  - Auch bei Delegation an Mitarbeiter: Kontrolle ist wichtig
  - Für Datenverlust haftet i.d.R. keine Versicherung
  - Für Datenverlust haftet (außer bei Vorsatz) i.d.R. auch kein IT-Dienstleister
  - **denn: Datensicherung ist oberste Anwenderpflicht**
- Prüfen Sie regelmäßig die Datensicherung
  - nicht nur Bänder wechseln
  - täglich Erfolg der Datensicherung per Plausibilitäts-Check prüfen
  - regelmäßig testweise Daten von den Medien zurücksichern
- Stellen Sie Notfallpläne für den Fall eines Datenverlustes auf
  - Feststellung der Ursache
  - Abstellen der Fehlerursache
- Dann erst Rücksicherung

Archivierungspflichten

Neben den nachvollziehbaren und auf der Hand liegenden Gründen, die für eine regelmäßige Datensicherung sprechen, gibt es zusätzlich auch allgemeine oder standes-rechtliche Regelungen und Gesetze, die eine Datensicherung (nämlich in Form einer Archivierung) vorschreiben.

- **Finanzamt**
    - Seit dem 1.1.2002 gilt als Aufbewahrungsfrist 10 Jahre für die Datenverarbeitungsanlage und die Bewegungsdaten, wenn der Unternehmer seine Rechnungen mit EDV-Hilfe erstellt.
- **Handelsrecht**
    - Nach Handelsrecht müssen Geschäftsbriefe und Schriftstücke ebenfalls 6 bis 10 Jahre aufbewahrt werden. Da heutzutage vielfach elektronisch kommuniziert wird, fallen darunter auch E-Mails. Vergessen Sie also ganz schnell die Idee, E-Mails einfach nach einiger Zeit zu löschen. Solange die Aufbewahrungspflicht noch nicht abgelaufen ist, müssen auch E-Mails aufbewahrt werden.
- **Datensicherung als Rating-Faktor**
    - Rating: Einstufung und Bewertung von Unternehmen durch die Kreditinstitute gem. BASEL II mit Einfluss auf die Konditionen für die Kreditvergabe
    - Rating-Verfahren berücksichtigt

        - „harte“ Faktoren wie z.B. Kapitaldecke, Verschuldungsgrad, Bonität etc.
        - „weiche“ Faktoren wie z.B. Alter der Geschäftsführung, **Datensicherungs- und Ausfallsicherungskonzepte für die IT**
- **Röntgenverordnung**
    - Aufbewahrung von (digitalen) Röntgenbildern 10 Jahre

Technische Herausforderung

Digital aufgezeichnete Daten über einen Zeitraum von 10 Jahren (oder länger) aufzubewahren, ist alles andere als eine triviale Aufgabenstellung. Ob eine handelsübliche Festplatte 10 Jahre funktioniert, ist schon einmal mehr als fraglich.

Es stellt sich also das Problem, ein Sicherungsmedium zu benutzen, welches aufgrund seiner physikalischen Eigenschaften überhaupt in der Lage ist, die Daten auch mindestens 10 Jahre speichern und mittels geeigneter Geräte auch nach Jahren wieder abrufbar machen zu können.

Ein Bandmedium scheidet daher für die Langzeitarchivierung über mehrere Jahre nach heutigen Erkenntnissen aus. Das Bandmaterial besteht aus einem Kunststoffträger, auf dem in einer aufgebrachten Magnetschicht kleinste Elementarmagnete enthalten sind, mit deren Ausrichtung die für die EDV verarbeitbaren Informationen „0“ und „1“ gespeichert sind. Durch die enge Wicklung des sehr dünnen Materials beeinflussen sich die Magnete nun mit der Zeit untereinander und verlieren so nach und nach die ursprüngliche Information (in der Fachsprache bezeichnet man den Effekt auch Übersprechen). Zudem ist das Material relativ anfällig gegenüber Hitze, Feuchtigkeit und mechanischer Belastung (z.B. beim Spulen).

Es heißt, die NASA hat vor Jahren einmal eine größere Menge Datenmaterial ihrer Apollo-Missionen verloren, als man Jahre nach der Speicherung diese nochmals abrufen wollte. Man hatte schlichtweg das Umspulen der Bänder vergessen. Also noch einmal zurück zum Mond fliegen und alles noch einmal aufzeichnen?

Es ist also wichtig, ein Langzeitarchiv mit Medien anzulegen, die nach Herstellerangaben und heutigen Erkenntnissen mindestens 10 Jahre Datensicherheit garantieren. Man hält in Fachkreisen CD- und DVD-Rohlinge hierzu nicht für ausreichend sicher, da die Lebensdauer der mit Brennern beschreibbaren Rohlinge mit höchstens 10 Jahren angesehen wird bzw. es hohe Streuverluste auch innerhalb derselben Charge geben kann. Die Medien sind nämlich neben der Empfindlichkeit gegen Kratzer auch einem Alterungsprozess durch UV-Licht ausgesetzt. Ein Backup auf CD/DVD könnte demnach also knapp nicht funktionieren.

Es gibt nur einige wenige Verfahren bzw. Medien, die nach heutigen Kenntnissen zu vertretbaren Kosten eine Langzeitarchivierung garantieren, die ihren Namen auch verdient hat. Dazu gehört u.a. die magnet-optischen Aufzeichnung. Solche MO-Medien sollen nach Herstellerangaben die enthaltenen Daten rund 60 Jahre halten können. Von daher ist der Einbau eines MO-Laufwerkes zur Langzeitarchivierung eine Überlegung wert. Alternativ dazu gibt es sogenannte M-Discs, spezielle DVD-Rohlinge, die laut Herstellerangaben sogar bis zu 1.000 Jahren funktionieren sollen und teilweise schon mit preiswerten DVD-Brennern beschrieben werden können. Über 1.000 Jahre sollen sogar sogenannte GlassMasterDiscs halten, die die Daten mit einem speziellen extrem widerstandsfähigen Glaswerkstoff einschließen. Last but not least, gibt es spezielle Flash-Speicher, die eine 100 Jahre Herstellergarantie aufweisen und rechnerisch sogar 1.300 Jahre halten sollen. Warten wir es ab.

Gegenüber Papier und gar Steintafeln sind die erreichbaren Speicherzeiten handelsüblicher EDV geradezu lächerlich kurz. Man denke mal daran, was wohl passiert wäre, wenn Moses die 10 Gebote mit dem Laptop aufgeschrieben oder Gutenberg die Bibel auf Facebook gepostet oder mit dem NTFS-Filesystem formatiert hätte…

Alternativ kann man natürlich auch dafür sorgen, dass steuerlich, handels- bzw. standesrechtlich relevante Dokumente durch regelmäßiges Umkopieren auf neue Medien / neue Systeme „am Leben gehalten werden“.

Das Finanzamt verlangt ebenfalls eine Langzeit-Archivierung und so kann man quasi als Nebeneffekt mit diesem System auch die Fakturierungs- und Buchhaltungs-Software zusätzlich z.B. mit dem Stand eines jeden Jahresabschlusses sichern und leistet somit den seit dem 1.1.2002 gültigen gesetzlichen Bestimmungen der Finanzbehörden Folge. Nach denen muss jeder, der gewerblich bzw. geschäftsmäßig mit einem elektronischen Datenverarbeitungssystem Leistungen abrechnet und Rechnungen erstellt, den Finanzbeamten bei einer Betriebsprüfung auf deren Verlangen den Zugriff auf die aktuelle EDV-Datenbestände und die vorangegangenen Bewegungs-Daten des Prüfzeitraumes ermöglichen. Für die Praxis bedeutet dies, dass jeder, der seine Rechnungen mit dem Computer erstellt, die Daten in einer lesbaren Form jeweils 10 Jahre lang nicht nur aufbewahren, sondern auch auswertbar bereitstellen muss. Wer die Schnelllebigkeit der Computerwelt und deren Standards kennt, kann einschätzen, welche technischen Probleme bei knallharter Auslegung der Bestimmung in Zukunft auf alle Gewerbetreibende zukommen werden. Auch nach 10 Jahren muss dann noch ein Computer vorhanden und betriebsbereit sein, um die „uralten“ Daten dem Finanzprüfer zur Verfügung zu stellen.

Ob die Finanzämter in der Praxis davon immer Gebrauch machen und ob die Beamten überhaupt in der Lage sein werden, die Vielzahl von Programmen zwecks Analyse der Bewegungsdaten bedienen zu können, sei wieder einmal dahin gestellt. Wer hier jedoch auf der sicheren Seite sein will, tut gut daran, sich hier frühzeitig ein handhabbares Konzept für den Fall der Fälle bereitzustellen. Und tatsächlich hatte der Autor kürzlich einen gutachterlichen Fall zu bearbeiten, bei dem es wegen einer Steuerprüfung und einer drohenden Nachzahlung im hohen sechsstelligen Bereich u.a. darum ging, Daten aus einem fünf Jahre zurückliegendem Wirtschaftsjahr wieder lesbar zu machen. Gut, dass der Steuerpflichtige in diesem Fall die Daten gesichert hatte.

Unter Berücksichtigung der vorangegangenen Datensicherungsmöglichkeiten mit Spiegelung, Bandsicherung und zusätzlicher Langzeitarchivierung erreicht man im Idealfall also ein dreistufiges Datensicherungskonzept. Das kann natürlich nie 100% vor einem Datenverlust schützen, die Wahrscheinlichkeit dafür jedoch auf ein absolut vertretbares und minimales Restrisiko reduzieren.

- Stufe 1: Spiegelung von Daten (Live) durch Einsatz von RAID-Systemen
- Stufe 2: regelmäßige Offline-Backups auf externe Medien (nicht dauerhaft angeschlossen bzw. im Zugriff)
- Stufe 3: Langzeit-Archivierung (durch geeignete Verfahren/Medien oder durch regelmäßiges Umkopieren der Sicherungsmedien)

Datenschutz

Was hat die Datensicherung (Datenspeicherung) mit Datenschutz zu tun?

Durch das Anfertigen von Backups werden (personenbezogene) Daten archiviert (Langzeit). Datensicherungen enthalten möglicherweise Daten, die im Original auf Anforderung des Betroffenen gelöscht wurden und Datensicherungen werden ggf. aus dem Haus an eine „sichere“ Stelle verbracht. Wer hat dann (später) darauf Zugriff?

Unter Datenschutz versteht man nicht den Schutz der Daten vor Verlust oder Zerstörung, sondern den Schutz von personenbezogenen Daten vor missbräuchlicher Nutzung durch die erfassenden Benutzer z.B. durch Erstellung von Nutzer- und Bewegungsprofilen mittels Cookies, RFID, Tracking usw. und den Schutz vor Weitergabe dieser Daten an nicht autorisierte Benutzer (Wahrung des Bank- oder Postgeheimnis, Wahrung der ärztlichen Schweigepflicht, Vermeidung unerwünschter Werbung uvm.).

Mit dem Werkzeug „Elektronische Datenverarbeitung“ (kurz EDV) sind die Begriffe „Datenschutz“ und „Datensicherheit“ eng verzahnt und gewinnen gerade in Bezug auf personenbezogene und unternehmenswichtige Daten einen immer größeren Stellenwert.

Viele Unternehmen und Institutionen sind ohne diese Daten in der heutigen, schnelllebigen und von riesigen Datenmengen geprägten Welt nicht mehr lebens- oder überlebensfähig.

Im Fall von personenbezogenen Daten kommt ein weiterer Aspekt hinzu. Die Person, über die die Daten erhoben worden sind, hat ein berechtigtes Interesse daran, dass diese Informationen nicht in fremde Hände fallen und unberechtigterweise ausgewertet oder weiterverarbeitet werden. Hier stößt man auf das weitläufige und zuweilen heiß diskutierte Thema „Datenschutz“.

Rechtlicher Ausgangspunkt ist das Grundrecht auf informationelle Selbstbestimmung. Die Grundidee ist, dass der Einzelne die Möglichkeit haben soll, selbst zu bestimmen, wer bei welcher Gelegenheit welche Informationen über ihn erhält. Als besonders gefährdend werden die Situationen angesehen, in denen große Organisationen Informationen - möglicherweise ohne Kenntnis der betroffenen Personen - sammeln, speichern und auswerten.

Gesetzliche Grundlagen: Das Bundesdatenschutzgesetz

Das Bundesdatenschutzgesetz vom 20.12.1990 wurde nach einer Überarbeitung im Jahr 2003 zuletzt am 05.02.2009 (Datum der Drucklegung) aktualisiert: *„Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.“ (§1 BDSG).*

Es regelt sowohl den sogenannten „öffentlichen Bereich“ (Bund, Länder und Kommunen, also die staatlichen Stellen) als auch den „nicht-öffentlichen Bereich“ (private Institutionen, Firmen, Vereine etc.).

Da jede Verarbeitung personenbezogener Daten durch öffentliche Stellen einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung darstellt, muss dafür im Einzelfall eine gesetzliche Erlaubnis vorliegen. Im privaten Bereich (in der Sprache der Datenschutzgesetze „nicht-öffentlicher Bereich“) existieren nicht so viele Regelungen. Diese sind in den meisten Fällen auch weniger konkret und lassen den Daten verarbeitenden Stellen mehr Freiheit. Ein rechtlicher Grund für diese Situation besteht darin, dass auch die privaten Stellen, die die Daten Dritter verarbeiten, sich dabei auf bestimmte Grundrechte (z.B. Berufsfreiheit) berufen können. Die datenschutzrechtlichen Regelungen sollen einen gerechten Ausgleich zwischen den unterschiedlichen Rechtspositionen herbeiführen.

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

§3 des BDSG besagt: *Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.*

Die Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung regelt §4 BDSG:
(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet ***oder der Betroffene eingewilligt hat****.*

(2) Personenbezogene Daten sind beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn

1. *eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt **oder***
2. *a) die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht **oder***
   b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

(3) Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über

1. *die Identität der verantwortlichen Stelle,*
2. *die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung **und***
3. *die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalls nicht mit der Übermittlung an diese rechnen muss, zu unterrichten.*

Werden personenbezogene Daten beim Betroffenen aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen ist er über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.

Zusammengefasst bedeutet dies, dass die oberste Prämisse die Vermeidung der Erhebung bzw. Speicherung von personenbezogenen Daten sein soll bzw., sofern dies nicht möglich ist, ansonsten die Datensparsamkeit an nächster Stelle steht. Dort, wo umsetzbar, soll von der Möglichkeit des Anonymisierens von Daten Gebrauch gemacht werden.

Der Betroffene hat das Grundrecht, von jeder verantwortlichen Stelle (also demjenigen, der die Daten erhoben, gespeichert oder verarbeitet hat) unentgeltlich Auskunft zu erhalten, welche Daten über ihn gespeichert sind und er kann verlangen, dass diese ggf. berichtigt oder gelöscht (gesperrt) werden. Besonderes Augenmerk ist bei der verantwortlichen Stelle dann walten zu lassen, wenn es sich um besonders schützenswerte personenbezogene Daten handelt. Das Gesetz benennt in §4d BDSG hierzu: *„rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben“.* Die Erhebung und Verarbeitung solcher Daten ist grundsätzlich nur dann zulässig, wenn eine sogenannte Vorabkontrolle durch den betrieblichen Datenschutzbeauftragten erfolgt ist bzw. sie ist ggf. meldepflichtig (bei der zuständigen Datenschutzbehörde).

Verwendung personenbezogener Daten

Die Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung für eigene Zwecke ist in §28 des BDSG geregelt:
(1) Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig,

1. wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient,
2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt ***oder***
3. wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt. Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen. (…)
(3) Die Übermittlung oder Nutzung für einen anderen Zweck ist auch zulässig:

1. *soweit es zur Wahrung berechtigter Interessen eines Dritten* ***oder***
2. *zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist* ***oder***
3. *für Zwecke der Werbung, der Markt- und Meinungsforschung, wenn es sich um listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt, die sich auf eine Angabe über die Zugehörigkeit des Betroffenen zu dieser Personengruppe, Berufs-, Branchen- oder Geschäftsbezeichnung, Namen, Titel, akademische Grade, Anschrift und Geburtsjahr beschränken und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat* ***oder***

4. *wenn es im Interesse einer Forschungseinrichtung zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.*

(4) ***Widerspricht der Betroffene*** *bei der verantwortlichen Stelle der Nutzung oder Übermittlung seiner Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung, ist eine Nutzung oder Übermittlung für diese Zwecke* ***unzulässig****.*

Zusammengefasst bedeutet dies, dass Firmen und Institutionen sehr wohl personenbezogene Daten ihrer Kunden speichern und verwenden dürfen, sofern es zur Vertragserfüllung notwendig ist. Dies werden regelmäßig neben Namen und Titel die postalische Adresse sowie z.B. Geburtsdatum und Bankverbindungen sein. Man soll dabei aber nur die Daten erheben und speichern, die man für die Pflege der Geschäftsbeziehung tatsächlich benötigt und hat die Verpflichtung, mit diesen sehr sorgfältig umzugehen (siehe dazu auch das nächste Kapitel). Auch das geschäftsmäßige Erheben und Handeln mit Adressen sowie daraus resultierend die Weitergabe an Dritte ist im BDSG (§29) geregelt.

Die Weitergabe an Dritte (Übermittlung) ist nur dann zulässig, wenn *a) der Dritte, dem die Daten übermittelt werden, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat oder b) es sich um listenmäßig oder sonst zusammengefasste Daten nach § 28 Abs. 3 Nr. 3 handelt, die für Zwecke der Werbung oder der Markt- oder Meinungsforschung übermittelt werden sollen und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.*

Zudem hat die Aufnahme personenbezogener Daten in elektronische oder gedruckte Adress-, Telefon-, Branchen- oder vergleichbare Verzeichnisse zu unterbleiben, wenn der entgegenstehende Wille des Betroffenen aus dem zugrunde liegenden elektronischen oder gedruckten Verzeichnis oder Register ersichtlich ist.

Grundsätzlich empfiehlt es sich also, die Betroffenen lieber einmal zu viel als zu wenig darüber aufzuklären, dass und welche personenbezogene Daten von ihnen gespeichert werden und sie um Erlaubnis zu fragen, bevor diese Daten in irgendeiner Form (die es erlaubt, einen Rückschluss auf die betreffende Person herzustellen) weitergegeben oder veröffentlicht werden. Neben dem Ärger mit einzelnen Betroffenen droht neben den zivil- und strafrechtlichen Konsequenzen ein erheblicher Imageschaden in der Öffentlichkeit.

Datenschutz bei Fernwartung

Auch das Thema Fernwartung ist unter dem Gesichtspunkt des Datenschutzes erneut zu beleuchten. Die Bundesärztekammer hat beispielsweise daher in ihren „Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“[3] u.a. festgestellt:

[3] [BÄK96] / http://lfd.m-v.de

Die Wartung einer EDV-Anlage oder jegliche Fehlerbeseitigung vor Ort darf grundsätzlich nur mit Testdaten erfolgen. Im Notfall, z. B. beim Systemstillstand in einer spezifischen Patientendatenkonstellation, muss der Einblick Dritter in Originaldaten auf besondere Ausnahmefälle eingeschränkt bleiben. Das Wartungspersonal ist zu beaufsichtigen und schriftlich auf die Verschwiegenheit zu verpflichten. Die durchgeführten Maßnahmen sowie der Name der Wartungsperson sind zu protokollieren.
Grundsätzlich gilt:

- *Die Fernwartung von EDV-Systemen in Arztpraxen ist unzulässig, wenn nicht auszuschließen ist, dass dabei auf patientenbezogene Daten zugegriffen werden kann.*
- *Bei einem Datenträgeraustausch mit befugten Dritten ist ein sicherer Transport zu gewährleisten.*
- *Die Datenfernübertragung personenbezogener Daten per Leitung muss chiffriert erfolgen.*
- *Auszumusternde Datenträger müssen unter Aufsicht des Arztes (z. B. durch mehrfaches Überschreiben mittels geeigneter Software) unbrauchbar gemacht werden.*

Betrieblicher Datenschutzbeauftragter

Ein weiterer in Bezug auf den Datenschutz zu beachtender Punkt ist, dass bei der automatisierten Verarbeitung von personenbezogenen Daten in einem Unternehmen, bei dem neun oder mehr Mitarbeiter mit diesen Vorgängen beauftragt sind, ein betrieblicher Datenschutzbeauftragter benannt werden muss, der die Einhaltung der Datenschutzrichtlinien überwacht. Diese gesetzliche Regelung trifft somit bereits für mittelgroße Unternehmen oder Praxen zu, bei denen mehrere Mitarbeiter regelmäßig Zugriff auf personenbezogene Daten haben. Bei erfassenden Stellen, die Daten verarbeiten, die einer Vorabkontrolle unterliegen, oder die mit Adressdaten handeln bzw. diese zu statistischen Zwecken nutzen, muss ein Datenschutzbeauftragter unabhängig von der Personenzahl installiert werden.

Der Datenschutzbeauftragte sorgt für die Schulung der Mitarbeiter in Bezug auf den vertraulichen Umgang mit personenbezogenen Daten, der Sensibilisierung für die sogenannte Datensparsamkeit (Sammeln nur wirklich benötigter Daten) und der Einhaltung der gesetzlichen und standesrechtlich relevanten Bestimmungen. Der Datenschutzbeauftragte muss dabei nicht aus der eigenen Praxis bzw. dem eigenen Unternehmen stammen, sondern kann als Dienstleistung z.B. über Standesorganisationen oder EDV-Sachverständige (wie z.B. der Autor Dipl.-Ing Thomas Käfer) hinzugezogen werden. Ausgeschlossen von der Arbeit als Datenschutzbeauftragter ist u.a. der Firmenchef bzw. Arzt selbst sowie der mit der Wartung der EDV-Anlage beauftragte Systemadministrator oder IT-Dienstleister (Vier-Augen-Prinzip).

Rechtsfolgen bei Missachtung des BDSG

Wird kein betrieblicher Datenschutzbeauftragter bestellt und/oder kommt es zu einer Datenschutzpanne, so kann das neben Schadensersatzansprüchen geschädigter Dritter gem. BGB und BDSG auch aufgrund der Verletzung von Sorgfaltspflichten (Aktien- und GmbH-Gesetz) Ansprüche der Gesellschafter an Vorstand und Geschäftsführer sowie strafrechtliche Konsequenzen (Ärzte, Steuerberater, Anwälte) nach sich ziehen. Der Image- und Vertrauensverlust ist aus den immer wieder publik werdenden Datenschutzpannen- oder missachtungen großer Firmen bekannt. Es können Bußgelder in Höhe bis zu 50.000 €, wenn kein Datenschutzbeauftragter bestellt oder tätig ist und bis zu 250.000 €, wenn tatsächlich ein Verstoß gegen das Datenschutzgesetz festgestellt wird (eine Schädigung eintritt), verhängt werden. In extremen Fällen sind sogar Freiheitsstrafen bis zu 2 Jahren möglich.

Aufgaben des Datenschutzbeauftragten

Der Datenschutzbeauftragte hat u.a. folgende Aufgaben:

- Schulung der Mitarbeiter hinsichtlich der Einhaltung des Bundesdatenschutzgesetzes (Datengeheimnis § 5 BDSG)

- Verpflichtung der Mitarbeiter zur Einhaltung des Datenschutzes
- Erstellung und Aktualisierung des „Verfahrensverzeichnisses für Jedermann"
- Erstellung und Aktualisierung der „internen Verarbeitungsübersicht"
- Durchführung von Vorab-Kontrollen
- Überwachung der ordnungsgemäßen Anwendung von Datenverarbeitungsprogrammen
- Überwachung der technisch-organisatorischen Maßnahmen
- Beantwortung konkreter Anfragen von Mitarbeitern zum Datenschutz
- Kontrolle, insbesondere durch Prüfung der Erforderlichkeit einer Vorabkontrolle und Durchführung der Vorabkontrolle (§ 4d Abs.5 BDSG); Hilfestellung am Arbeitsplatz
- Prüfung der Einhaltung der datenschutzrechtlichen Erfordernisse in der Betriebskommunikation
- Auskunfts- und Registeraufgaben, insbesondere durch Auskunftserteilung gegenüber Betroffenen
- Verwaltung der Verfahrensverzeichnisse für die Bereiche, die personenbezogene Daten verarbeiten
- Auskunft über etwaige Meldepflichten der verantwortlichen Stelle
- Optimierung der technischen und organisatorischen Abläufe der Datenerhebung und -verarbeitung, insbesondere durch Erstellung und Pflege der Datenschutz-Dokumente (z.B. öffentliches Verfahrensverzeichnis, Verfahrensbeschreibung/ interne Verfahrensübersicht, Datenschutzkonzeption, notwendige Dokumentationen für automatisierte Abrufverfahren, Definition und Dokumentation technischer und organisatorischer Maßnahmen bei der Auftragsdatenverarbeitung)

- Unterstützung der Durchsetzung unternehmerischer Entscheidungen, insbesondere durch Prüfung auf Konformität mit datenschutzrechtlichen Vorschriften; ggf. Entwicklung von Alternativlösungen, die datenschutzrechtlich unbedenklich und betriebswirtschaftlich möglichst wenig aufwendig sind
- öffentlichkeitswirksame Darstellung von Datenschutzmaßnahmen

Datenschutzrichtlinien

Da personenbezogene Daten besonders schützenswert sind und die verantwortliche Stelle vom Gesetzgeber eine besondere Sorgfaltspflicht auferlegt bekommen hat, dass die Daten u.a. nicht in fremde, unbefugte Hände gelangen, hat die Datenübermittlung (an Dritte) auf einem sicheren Weg zu erfolgen.

Es verbietet sich daher, personenbezogene Daten gesammelt als Liste oder auch einzeln auf ungesicherten Wegen zu übertragen. Dazu gehört insbesondere die Übertragung per E-Mail. E-Mail-Kommunikation ist in der Regel vollkommen unverschlüsselt und kann von Fremden mit geringem Aufwand mitgelesen (und verfälscht) werden. Ein Versenden solcher Daten, vor allem dann, wenn es sich auch noch um besonders schützenswerte personenbezogene Daten (vgl. §4d BDSG) handelt, ist daher aus Sicht des Autors nur über eine verschlüsselte Nachrichtenübertragung zu gewährleisten. Hierzu kann man sich z.B. freier Systeme mit sogenannten Public-Key-Infrastrukturen wie z.B. PGP[4] bedienen.

Auch die Versendung solcher Daten mit der üblichen Briefpost ist nicht unkritisch. Hier gilt zwar das Postgeheimnis (im Gegensatz zur E-Mail-Kommunikation), jedoch ist über diesen Weg noch nicht sicher gestellt, dass der Empfänger die personenbezogenen Daten tatsächlich auch erhalten hat.

[4] PGP: Pretty Good Privacy - von Phil Zimmermann entwickeltes Programm zur Verschlüsselung und zum Unterschreiben von Daten

Hier hilft nur ein Einschreiben mit Rückschein als Nachweis oder ein mit dem Empfänger ausgehandeltes Verfahren (z.B. einer Ankündigung des Versenders über eine bevorstehende Sendung und nachfolgend einer Bestätigung des Empfängers per E-Mail, dass die Daten per Post angekommen sind). Sobald eine große Menge personenbezogener Daten an einen Dritten (immer unter Berücksichtigung der Zulässigkeit) übermittelt (transportiert) werden soll, sollte dies z.B. auf CD-ROM gespeichert über verlässliche Kuriere oder persönlich erfolgen. Solche Datensammlungen darf man nie ungesichert per E-Mail (als Zip-Anhang) verschicken oder ungeschützt auf einer Web-Seite zum Download ablegen.

Datenschutzempfehlungen

- Datensparsamkeit!
    - Erheben Sie nur die Daten, die Sie wirklich brauchen (z.B. Geburtsdatum, Haarfarbe, Personalausweis-Nr.)
    - Brauchen Sie diese Daten für Ihre Arbeit wirklich?
    - Sorgen Sie für einen auf das Mindestmaß beschränkten Zugriff auf die Daten (Kreis der Benutzer)
    - Geben Sie nicht Ihre Benutzerkennungen/Passwörter weiter (auch nicht an Kollegen)
    - Keine personenbezogenen Daten preisgeben / Fremden zugänglich machen!
    - Daten sicher vernichten (wenn nicht mehr benötigt oder auf Aufforderung des Betroffenen)
    - Informieren Sie die Betroffenen lieber einmal zu viel als zu wenig über die Speicherung ihrer Daten und ihrer Rechten
- Bei Zweifeln:
    - Schauen Sie in die von Ihrem Datenschutzbeauftragten erstellte Handreichung zum Thema Datenschutz (Verfahrensverzeichnis)
    - Schauen Sie ins Gesetz (BDSG)

    - Fragen Sie Ihren Datenschutzbeauftragten
    - Bei Anfragen von außen zum Thema Datenschutz: Beantworten Sie Fragen von Betroffenen offen und ehrlich. Sie haben nichts zu verbergen!
    - Bei unklaren Sachlagen: Fragen oder verweisen Sie an den betrieblichen Datenschutzbeauftragten (datenschutz@firma.de). Der Betroffene hat das Recht, sich mit dem Datenschutzbeauftragten in Verbindung zu setzen!
    - Nehmen Sie Anfragen oder Aufforderungen von Betroffenen zum Thema Datenschutz ernst. Es kann sonst großer Schaden in Bezug auf Haftung, Schadensersatz, Bußgeldern und Image (!) entstehen.
- Im Konfliktfall
    - bei externen Betroffenen
    - bei internen Datenschutz-Konflikten zwischen Kollegen oder mit dem Chef

Informieren Sie umgehend den betrieblichen Datenschutzbeauftragten!

Merke: Der betriebliche Datenschutzbeauftragte ist Anwalt der Betroffenen und Mittler zwischen den Akteuren!

Datensicherheit

Wenn Ihre Daten erfolgreich gegen Verlust durch technische Probleme gesichert und diese Daten auch noch unter Beachtung des Datenschutzes erfasst und gespeichert worden sind, dann brauchen Sie sich „nur noch“ um das Thema „Datensicherheit“ zu kümmern. Hier geht es tatsächlich um alle Angriffe auf Ihre Daten von innen und außen (sowohl aus Unternehmens- als auch Netzwerk-Sicht gesehen), die darauf abzielen, diese mitzulesen, zu stehlen, zu verändern oder zu löschen.

Ein beliebter Angriffspunkt für Datendiebstahl bzw. -kompromittierung ist das Medium E-Mail und daher nähern wir uns dem Thema über das digitale signieren und verschlüsseln von Daten.

Digitale Signatur und Verschlüsselung

Im Geschäfts- wie im Privatleben hat sich das Medium „E-Mail“ als leistungsfähiges und effektives Kommunikationsmittel etabliert. So werden hierüber Informationen, Dateien und Nachrichten ausgetauscht, Verabredungen getroffen, Aufträge erteilt und Verträge geschlossen.

Was vielen Nutzern dabei nicht bewusst ist, ist, dass dieser E-Mail-Verkehr nicht nur mitgelesen (abgehört) werden kann, sondern auch, dass Teile der E-Mail oder die E-Mail komplett gefälscht werden können und der tatsächliche Absender nicht derjenige sein muss, der in der E-Mail als vermeintlicher Versender hinterlegt ist.

Hieraus resultieren ernsthafte wirtschaftlich und rechtlich relevante Konsequenzen. Aufgrund der Tatsache, dass der komplette E-Mail-Verkehr gefälscht werden kann, gilt dieser vor Gericht i.d.R. nicht als Beweis.

Möchte eine Streitpartei also beweisen, dass die gegnerische Seite eine bestimmte Aussage getätigt hat, so kann hierzu kaum eine entsprechende E-Mail als anerkannter Nachweis herangezogen werden. Selbst das übliche Zitieren der Originalnachricht bei einer Antwort (Reply) dient zwar in der Praxis als gern genutztes Feature, um den Gesprächsverlauf auch im Nachhinein nachvollziehen zu können, jedoch ist auch eine solche E-Mail-Kette (Thread) manipulierbar und damit als Beweis wertlos, hilft aber immerhin noch als Indiz (besser als gar keine Aufzeichnung).

Die rechtliche Anerkennung einer E-Mail scheitert also an zwei Punkten: Erstens ist der Inhalt einer E-Mail teilweise oder komplett fälschbar und zweitens ist der Absender der E-Mail nicht zweifelsfrei zu identifizieren bzw. einer natürlichen Person zuzuordnen.

Fragen Sie sich einmal:

- Können Sie sicher sein, dass eine E-Mail, die Sie erhalten haben, auch tatsächlich von dem Absender stammt, der in der Nachricht angegeben ist?
- Können Sie sicher sein, dass diese E-Mail nicht mitgelesen wurde?
- Können Sie sicher sein, dass diese E-Mail unverfälscht bei Ihnen angekommen ist?

Die Antwort auf alle drei Fragen lautet: NEIN!

Ärgernis SPAM

Es ist sehr einfach, an eine anonymisierte E-Mail-Adresse zu gelangen. Hierzu gibt es genügend Internet-Dienste, die - rein auf Werbebasis finanziert - Privatleuten einen kostenlosen E-Mail-Account anbieten. Die Legitimationsprüfungen bei Anlage einer solchen E-Mail-Adresse sind auf einfache Weise zu umgehen. Hierdurch kann der sich Nutzer dieser E-Mail-Adresse vollkommen anonym im Medium Internet bewegen.

Es müssten nun mit diesem Account schon sehr schwerwiegende Rechtsverstöße begangen werden, damit der erhebliche Aufwand betrieben würde, anhand der in den E-Mails hinterlegten Routen-Informationen über die beteiligten Internet-Provider den Weg bis hin zum Absender-PC zurückzuverfolgen. Da hierzu auch ein anonym zu nutzender Internet-Café-Rechner benutzt worden sein könnte, wird die Zuordnung zu einer bestimmten Person schwierig bis unmöglich.

Professionelle Spammer nutzen zum Versenden ihrer Werbe-E-Mails sogar illegal und oft unbemerkt fremde Rechner und verwischen ihre Spuren in der Regel so gut, dass der Ursprung einer solchen Werbe-E-Mail nicht zurückverfolgt werden kann.

Der Feind hört mit

Aber selbst wenn ein Benutzer einen regulären E-Mail-Account nutzt und sich in seiner elektronischen Nachricht durch Angabe von Name und Postadresse zu erkennen gibt, ist er selber nicht sicher davor, dass seine E-Mail auf dem Weg zum Empfänger verfälscht oder mitgelesen werden kann. E-Mails werden standardmäßig vollkommen unverschlüsselt im Klartext verschickt und liegen für kurze Zeit immer wieder auf den am Transport der Nachricht beteiligten Systemen der einzelnen Internet-Dienstleister. Durch gezieltes Abhören des Datenstroms oder unerlaubte Zugriffe auf die Postfächer mit den dort als Datei gelagerten E-Mails ist es also möglich, den Inhalt mitzulesen und, eine geeignete Infrastruktur oder Zugriffsrechte vorausgesetzt, diese auch zu verändern (oder die Zustellung ganz zu unterbinden).

Um diese Probleme zuverlässig zu beheben, bedarf es zweier Mechanismen: Erstens müssen E-Mails so gekennzeichnet werden, dass bereits die minimalste nachträgliche Manipulation angezeigt werden kann und zweitens müssen die E-Mails so verschlüsselt werden, dass nur der legitimierte Empfänger diese wiederum entschlüsseln kann.

Fast Facts

- E-Mail-Verkehr ist i.d.R. vollkommen unverschlüsselt
- Der Weg der E-Mails ist unbestimmt
- E-Mails lagern für kurze Zeit auf verschiedenen, fremden Rechnern (Server der beteiligten Provider)
- Provider müssen bestimmte Daten für eine gewisse Zeit für Strafverfolgungsbehörden speichern

Nutzen Sie für die Übertragung geheimer, unternehmenskritischer oder schützenswerter personenbezogener Informationen nie unverschlüsselte E-Mails!

Abhilfemaßnahmen

- Digitale Unterschrift
    - sichert die Authentizität der Nachricht
        - Der Absender lässt sich identifizieren
        - Der Empfänger kann erkennen, ob eine Nachricht verfälscht wurde
        - Der Empfänger kann NICHT erkennen, ob die Nachricht mitgelesen wurde
- Verschlüsselung
    - sichert den Inhalt der Nachricht.
        - Das Mitlesen wird verhindert
        - Das Verändern der Nachricht wird verhindert
        - Der Empfänger kann NICHT zweifelsfrei erkennen, von wem die Nachricht stammt

Das Anzeigen einer Datenmanipulation kann man dadurch erreichen, dass man eine elektronische Nachricht oder auch eine Datei digital signiert. Hierbei wird aus den Daten der Originalnachricht zusammen mit einem speziellen Schlüssel eine Prüfsumme gebildet (Hash-Wert) und mit der E-Mail oder Datei abgespeichert.

Wird nun die Nachricht nachträglich verändert, so passt der beim Empfang der E-Mail ebenfalls errechnete Hash-Wert nicht mehr mit der übermittelten Prüfsumme überein. Somit ist das Siegel „zerbrochen“ und die Nachricht wird entsprechend als kompromittiert gekennzeichnet.

Nun hat der Gesetzgeber im Jahr 2002 das sogenannte Signaturgesetz verabschiedet, in dem die digitale Signatur der natürlichen Unterschrift bis auf bestimmte Ausnahmefälle (z.B. Grundstückskauf) rechtlich gleichgestellt wird.

Auch wenn der technischen Umsetzung dieses Gesetzes in der Praxis bisher nicht die Bedeutung beigemessen worden ist, wie vielleicht gewünscht oder erwartet, so gibt es zwischenzeitlich jedoch Lösungen, um elektronisch zu signieren.

Man unterscheidet hierbei grundsätzlich zwei Formen der Signatur: eine un- oder nicht-qualifizierte Signatur und eine qualifizierte Signatur jeweils mit zwei Unterformen. Eine nicht-qualifizierte Signatur genügt nur niedrigen Sicherheitsanforderungen bzgl. der Herausgabe und der Überwachung eines Zertifikates und ist daher für die meisten rechtlich relevanten Geschäftsprozesse vollkommen uninteressant. Der konzeptionell schwache Schutz einer unqualifizierten elektronischen Signatur schlägt sich in der Praxis durch die geringe Akzeptanz und die eingeschränkte Verwendbarkeit bei wirklich interessanten Transaktionen nieder. Darüber kann dann auch nicht das vergleichsweise einfache Verfahren zum Erwerb einer solchen Signatur hinwegtrösten (das ist ja gerade das Problem). Zum Erhalt einer qualifizierten Signatur bedarf es daher eines deutlich höheren administrativen Aufwands zur Prüfung der Legitimation des Beantragens eines Zertifikates und dies ist auch mit entsprechenden Kosten verbunden.

Ohne Zertifikatsgeber keine Verifikation der Signatur

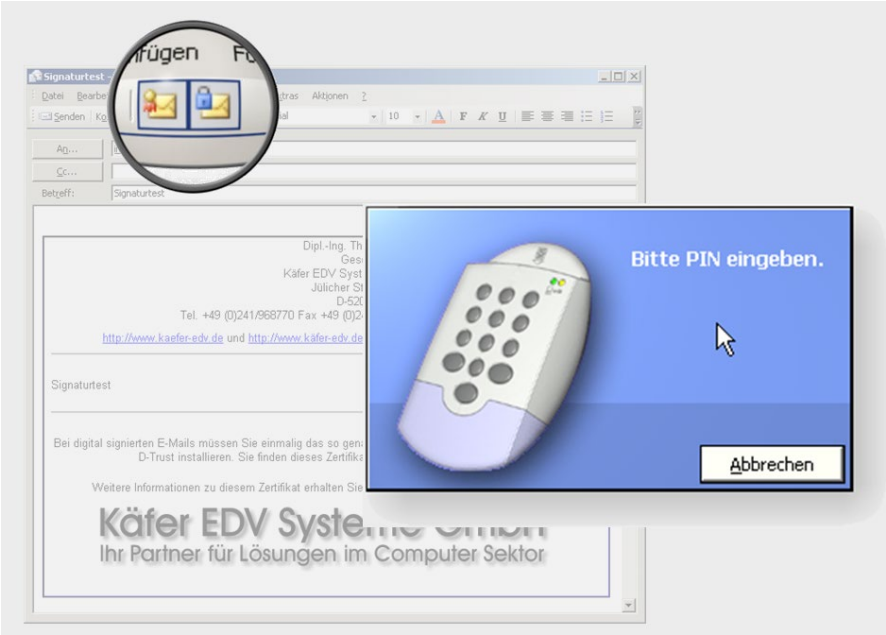
Grundsätzlich müssen sich alle Zertifikatsgeber (Trust-Center) bei der Regulierungsbehörde für Telekommunikation und Post (kurz RegTP[5]) zertifizieren lassen. Über die RegTP erhält man daher auch eine aktuelle Liste der registrierten Zertifikatsgeber, ohne dass diese eine besondere Empfehlung für den einen oder anderen Anbieter ausspricht. Hat man sich für einen Anbieter entschieden, so beantragt man als natürliche Person oder Institution eine qualifizierte Signatur auf dem Schriftweg. Da im Fall einer natürlichen Person die elektronische Signatur eindeutig zugeordnet werden soll, muss der Herausgabe eine persönliche Identitätsprüfung vorausgehen. Dies erfolgt, je nach Anbieter, durch das persönliche Abholen der Signaturkarte und Legitimation per Ausweisdokument an zentralen Stellen (z.B. teilnehmende IHK) oder z.B. per Post-Ident-Verfahren, bei dem der Antragsteller sich gegenüber einem Mitarbeiter der Deutschen Post am Schalter legitimiert. Somit soll sichergestellt werden, dass man nicht anonym in den Besitz einer qualifizierten Signatur gelangen kann.

Technische Realisation

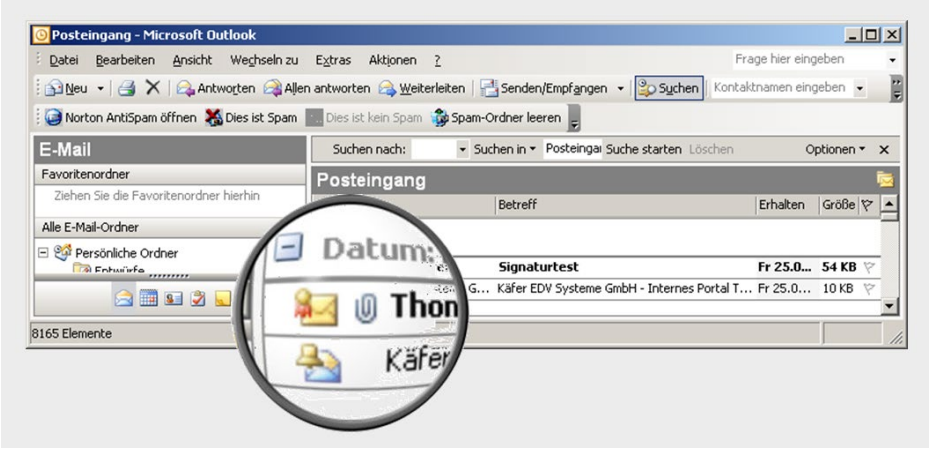
Technisch wird das Signieren so gelöst, dass an den PC ein Kartenlesegerät angeschlossen wird, in das die Signaturkarte eingesteckt wird. Dann werden einmalig entsprechende Treiber und Anwendungsprogramme bzw. Plug-Ins installiert, mit deren Hilfe man das auf der Karte enthaltene Zertifikat nutzen kann. Beim Versenden von Nachrichten z.B. mit Outlook® kann als Option die Nachricht mit diesem Zertifikat signiert werden.

---

[5] siehe http://www.regtp.de/



Der Empfänger erkennt eine signierte Nachricht an einem speziellen Symbol, welches nach Anklicken entsprechende Informationen über die Signatur preisgibt.



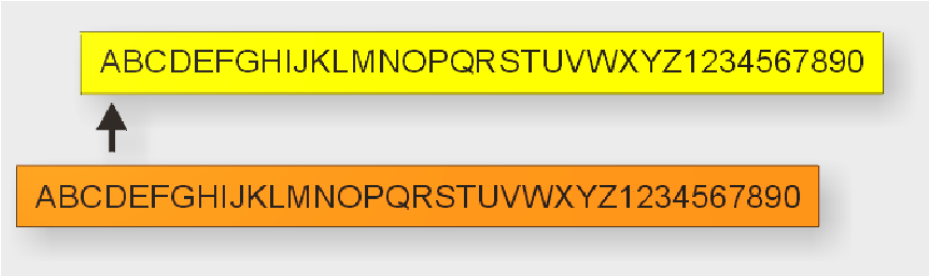
So lässt sich erkennen, ob die Signatur gültig und die Nachricht unverfälscht eingetroffen ist. Wurde auf dem Weg vom Sender zum Empfänger auch nur ein einziges Byte verändert, so ist die Signatur ähnlich wie bei einem klassischen Siegel zerbrochen. In der Praxis hat das Signieren von E-Mails einen gewissen Handling-Nachteil. So muss der Versender i.d.R. bei jedem Abschicken einer Nachricht eine PIN am Kartenterminal zur Freigabe eingeben und beim Empfänger muss das Zertifikat des verwendeten Trust-Centers installiert sein. Sofern sich das Trust-Center nicht bei den betreffenden Herstellern bereits authentifiziert hat (z.B. bei Microsoft®), „kennt“ das Empfängersystem das Zertifikat der eingehenden E-Mail nicht und es muss daher manuell installiert werden. Erst danach ist eine Online-Überprüfung automatisiert möglich, die es dem Empfänger erlaubt, die Gültigkeit der verwendeten Signatur zu überprüfen. Es liegt in der Natur der Sache, dass primär der Empfänger signierter Nachrichten einen Vorteil erhält (nämlich, dass er sich sicher sein kann, dass die empfangene E-Mail tatsächlich von dem angegebenen Sender stammt und diese nicht verfälscht wurde), der Sender jedoch den Aufwand und die Kosten trägt. Dies ist sicherlich ein Grund, warum die digitale Signatur bisher keine massenhafte Verbreitung erfahren hat. Es ist jedoch erstrebenswert, dass es sich zumindest im geschäftlichen Umfeld einbürgert, Nachrichten zu signieren, um neben der gewünschten Rechtssicherheit auch das Problem SPAM zu lösen.

Ein an und für sich vielversprechender Ansatz ist der „neue“ Personalausweis im Checkkartenformat, der auf Wunsch des Ausweisinhabers mit Funktionen zur digitalen Identifizierung ausgestattet (freigeschaltet) wird. Leider ist dieses Verfahren nicht sicher und die seit der Einführung bekannten Sicherheitslücken mit Stand der Drucklegung (Mai 2013) immer noch nicht behoben.

Verschlüsselung

Das digitale Signieren löst aber nur das eine der beiden Probleme, nämlich das Erkennen, ob eine Nachricht unverfälscht oder manipuliert empfangen wurde. Auch eine digital signierte E-Mail ist weiterhin im Klartext für jedermann lesbar. Dieses Problem löst somit erst das Verschlüsseln (Chiffrieren) der Nachrichten.

Symmetrische Verschlüsselung



Ein einfaches Verfahren (auch bekannt als Cäsar-Algorithmus), um Nachrichten zu verschlüsseln, kennen viele sicherlich noch aus der Kindheit. Hier hat man die Buchstaben einfach um eine bestimmte Anzahl von Stellen nach hinten im Alphabet verschoben. Bei einem Versatz z.B. um drei Zeichen wird aus einem A ein D, aus einem B ein E usw..

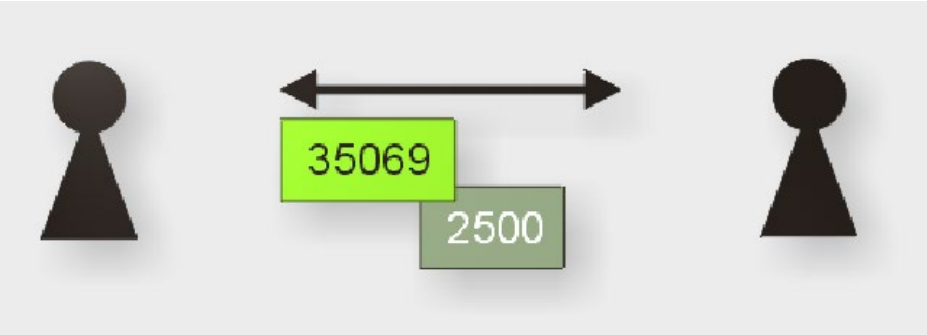
Der Empfänger der Nachricht muss hierbei also nur wissen, um wie viele Stellen er die Zeichen wieder nach vorn im Alphabet verschieben muss, um die Information im Klartext lesen zu können.

Den Informationsaustausch über die Anzahl der Stellen, um die die Buchstaben verschoben werden müssen (entspricht dem Schlüssel), bezeichnet man als Schlüsselaustausch. Das klassische Verfahren nutzt dabei den gleichen Schlüssel für Ver- und Entschlüsselung. Man bezeichnet dies daher als symmetrisches Verfahren. Zur Entschlüsselung muss der Empfänger also stets den gleichen Schlüssel besitzen, der zuvor über ein sicheres Medium (z.B. Kurier) ausgetauscht wurde. Keinesfalls darf der geheime Schlüssel nun über das gleiche, unsichere Medium übertragen werden, wie die Nachricht selbst, da sonst ein Lauscher die verschlüsselte Nachricht problemlos entschlüsseln könnte.

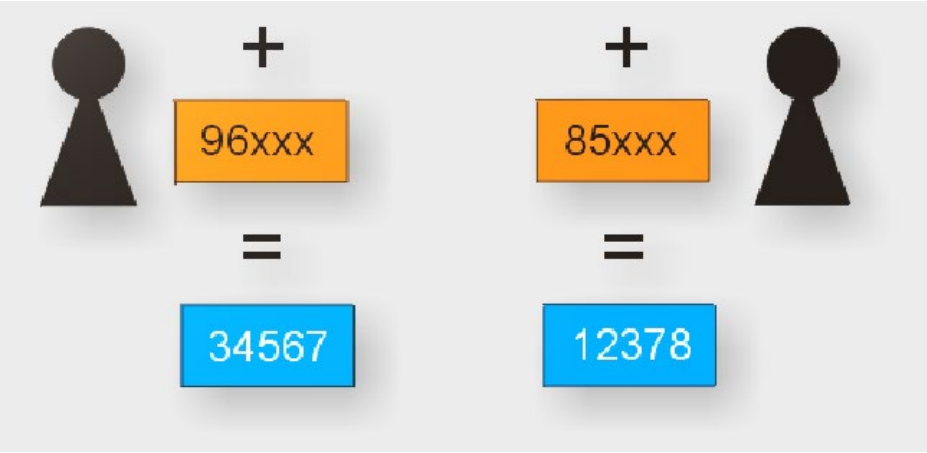
Asymmetrische Verschlüsselung

In der Praxis haben sich daher in der neueren Geschichte sogenannte asymmetrische Verfahren zur Verschlüsselung bewährt. Hierbei existiert jeweils ein Schlüsselpaar, bestehend aus einem privaten, geheimen und einem öffentlichen Schlüssel (Private und Public Key). Das Verfahren, welches auf Diffie-Hellman zurückgeführt wird, funktioniert dabei wie folgt:

Beide Kommunikationspartner einigen sich auf zwei Zahlen, eine große Primzahl sowie eine ganze Zahl, die kleiner als die Primzahl sein muss. Der Austausch dieser beiden Zahlen kann öffentlich erfolgen und hat keinen Einfluss auf die Sicherheit.

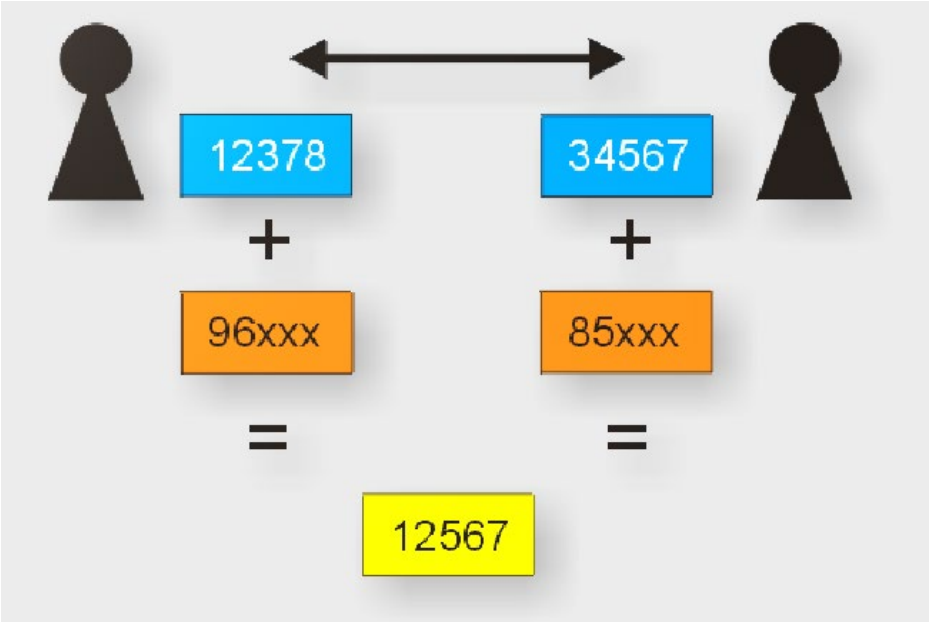


Dann generiert jeder eine weitere, geheime Zahl (Private Key).



Anschließend wird eine Berechnung mit dem Private Key und den vorher ausgetauschten beiden Zahlen durchgeführt, welches im Ergebnis den Public Key darstellt.

Nach gegenseitigem Austausch der beiden Public Keys führen sie jeweils eine private Berechnung für den eigenen Private Key und den Public Key des Kommunikationspartners durch. Die Zahl, die sich daraus ergibt, ist der Session-Key (ist für beide Partner gleich).



Der Session-Key kann nun als geheimer Schlüssel für einen anderen Verschlüsselungsalgorithmus, wie z.B. DES/3DES o.ä., genutzt werden. Ohne Kenntnis eines der beiden Private Keys kann nun kein Dritter an den gleichen Session-Key und damit zum Schlüssel zum Dechiffrieren der Nachricht gelangen. Der große Vorteil des Verfahrens ist, dass ein Beobachter auch in Kenntnis beider öffentlicher Schlüssel die Nachrichten nicht dechiffrieren kann. Die verwendeten mathematischen Verfahren lassen sich sehr leicht vorwärts, aber nur sehr schwer rückwärts rechnen.

Falltür-Algorithmus

Man bezeichnet so etwas auch als „Falltür-Algorithmus“ der nur in eine Richtung funktioniert. Vergleichbar ist das mit auch mit einem Fleischwolf: Wenn Sie ein Schwein durch einen Fleischwolf drücken, kommt Hackfleisch heraus.

Drücken Sie das Hackfleisch nun wieder zurück durch den Fleischwolf und lassen Sie selbigen rückwärts laufen, werden Sie oben kein Schwein herausbekommen.

Okay, das Beispiel ist jetzt etwas blutig und nicht für Vegetarier geeignet, aber anschaulich, oder?

Verglichen (z.B. bei einer Passwort-Verifizierung) wird tatsächlich jeweils nur der Hash (also das Hackfleisch). Ein identisches Schwein wird mit demselben Fleischwolf (analog zum Schlüssel für die Codierung) immer identisches Hack (Hash) erzeugen. Vorteil: Man braucht nicht das eigentliche Passwort (hier wieder das Schwein) abzuspeichern, zu übertragen bzw. preiszugeben, sondern nur den Hash-Wert. Vom Hash-Wert auf das Passwort zu schließen ist durch reines Zurückrechnen unmöglich.

Virtual Private Networks (VPN)

Anwendung findet eine solche Verschlüsselung z.B. in sogenannten VPN's, bei denen mit Hilfe der Kryptografie die zu transportierenden Daten an den Kopfstellen der Kommunikationspartner so verschlüsselt werden, dass für den Datentransport ein unsicheres, offenes Medium wie z.B. das Internet genutzt werden kann und die Daten auf ihrem Weg nicht oder nur erschwert durch Dritte mitgelesen werden können.

Hybride Verfahren

Die symmetrische und die asymmetrische Verschlüsselung haben beide ihre Vor- und Nachteile: Das symmetrische Verfahren arbeitet deutlich schneller, jedoch ist zur Verschlüsselung und zur Entschlüsselung derselbe Schlüssel notwendig, was zum einen ein Missbrauchsszenario (nämlich beim Empfänger, der nun seinerseits Daten mit dem fremden Schlüssel verschlüsseln und sich gegenüber Dritten als der Besitzer des Schlüssels ausgeben könnte) und zum anderen das Problem eröffnet, den Schlüssel erst einmal auf sicherem Wege zu übertragen.

Das asymmetrische Verfahren arbeitet langsamer, kennt hingegen aber nicht das Problem, dass der Schlüssel zum Verschlüsseln auf geheimem Weg übertragen werden muss, da er ja öffentlich bekannt ist (sein darf).

Man kombiniert daher in der Praxis oft beide Verfahren, um die Vorteile zu nutzen und die Nachteile zu eliminieren. Bei der Hybrid-Verschlüsselung wird zunächst der symmetrische Schlüssel mit einem asymmetrischen Verfahren gesichert übertragen (zwischen den Kommunikationspartnern ausgetauscht) und dann mit der schnelleren symmetrischen Verschlüsselung die eigentliche Datenübertragung durchgeführt.

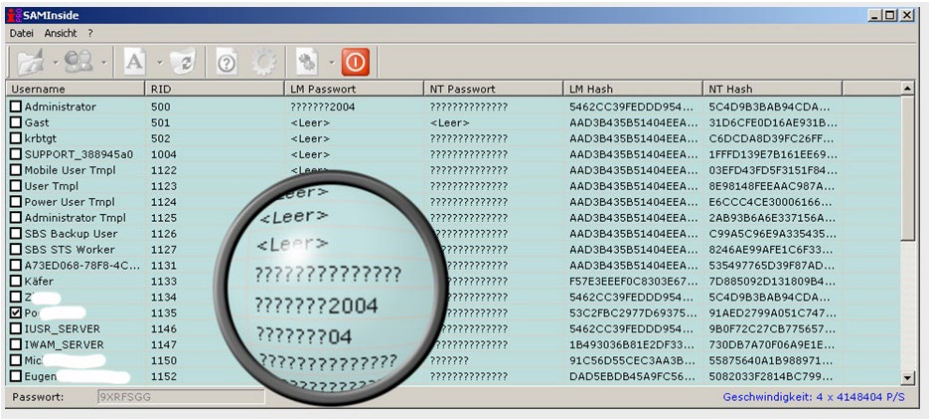
Übrigens: Ein beliebter Fehler ist es, „Asymmetrisch und Symmetrisch" mit „Asynchron und Synchron" zu verwechseln. Das eine hat mit dem anderen nichts zu tun.

Angriffsszenarien

Brute-Force-Attacken

Selbstverständlich sind prinzipiell alle Verschlüsselungsverfahren spätestens durch sogenannte Brute-Force-Attacken (mit „brutaler Gewalt“) zu knacken, jedoch bedarf es bei modernen Verfahren und entsprechend großen Verschlüsselungstiefen (z.B. > 128 BIT) sehr viel Rechenzeit, so dass solche Attacken in der Praxis nicht immer in einem realistischen Zeitrahmen durchführbar sind.

Passwort-Sicherheit



Erst durch gezieltes Ausnutzen von konzeptionellen oder von Benutzern verursachten Schwachstellen wird eine Brute-Force-Attacke zum Ziel führen. Ein Beispiel dafür ist z.B. das Knacken von Windows Passwörtern. Vor allem ältere Windows®-basierende Clients speichern Benutzerpasswörter in einem sehr unsicheren LANMAN-Hash-Format. Solche Passwörter werden wie bei UNIX auch nie im Klartext auf einem Server gespeichert, sondern im sogenannten HASH-Format. Windows LanMan-Passwörter können max. 14 Zeichen lang sein und werden in zwei Teilen á 7 Zeichen gespeichert. Kürzere Passwörter werden vom System aufgefüllt.

Da der Zeichenvorrat relativ begrenzt ist, bei den alten Windows-Versionen grundsätzlich nicht zwischen Groß- und Kleinschreibung unterschieden wird und die Benutzer sehr oft triviale Passwörter wählen, ist eine Brute-Force-Attacke, wenn sie mit Zugriff auf die Passwortdatenbank erfolgen kann, in der Praxis mit Programmen für rund 40,- € (oder kostenlos) eine Frage von wenigen Minuten. Oft werden nämlich Teile des Passwortes mit einer Wörterbuch-Attacke dechiffriert, so dass man sich nachfolgend mit einer Brute-Force-Attacke nur noch auf wenige Zeichen beschränken muss oder Reststücke erraten werden können. Als Abhilfe ist es daher ratsam, bei Windows 2000 oder XP-Systemen den LANMAN-Hash über die Registry zu deaktivieren.

Übrigens: Wer Spaß daran hat, einmal eine (fiktive) Story zu diesem Thema zu lesen und zu erfahren, wie man aus einem einfachen Passwort-Knacken einen spannenden und kurzweiligen Krimi mit Technik, weltweiter Verschwörung, organisierter Kriminalität, Gut und Böse, Liebe (kurz alles, was zu einer guten Story gehört) macht, dem sei der Krimi „Praha“ von Thomas Käfer empfohlen (https://www.kaeferlive.de/web/praha). Den ersten Toten gibt es übrigens bereits auf Seite 1. Viel Spaß beim Lesen.

Bei der Passwortwahl sollte man darauf achten, dass die Passwörter aus Buchstaben, Zahlen und Sonderzeichen zusammengesetzt werden, möglichst lang sind und natürlich nur an äußerst sicheren Stellen hinterlegt werden dürfen (nicht mit einem Zettel am Bildschirm oder unter der Tastatur). Eine gute Hilfestellung zum Merken von Passwörter ist es, die Anfangsbuchstaben der Wörter eines Liedtextes (incl. Satzzeichen) zu verwenden: „Hoch auf dem gelben Wagen, sitz ich beim Schwager vorn.“ ergibt als Passwort z.B. „HadgW,sibSv.“ oder „Ein Jäger aus Kurpfalz.“ ergibt „1JaK.“ usw.. Besser noch: Denken Sie sich einen eigenen Satz aus, den Sie sich gut merken können, der aber nicht Allgemeingut ist.

Nach heutigen Maßstäben und den technischen Möglichkeiten zum maschinellen Knacken von Zugangskennungen muss ein Passwort mindestens zehn Zeichen haben, aus Buchstaben (Groß-/Kleinschreibung), Zahlen und Sonderzeichen bestehen und darf in keinem Wörterbuch zu finden sein. Je größer der Zeichenvorrat ist, aus dem ein Passwort aufgebaut ist (werden kann), umso größer ist die Anzahl der möglichen Kombinationen und damit die benötigte Zeit, um diese alle durchzuprobieren. Mit der heutzutage (i.d.R.) verfügbaren Rechenleistung liegt die Grenze, bei der mit einer Brute-Force-Attacke ein Passwort entschlüsselt werden kann, zwischen 8 und 9 Zeichen. Das liegt daran, dass mit jedem zusätzlichen Zeichen der Rechenaufwand für die hinzu kommenden Möglichkeiten ab etwa der 8. Stelle exponentiell anwächst. Passwörter ab 10 Zeichen Länge gelten daher derzeit als sicher, sofern sie nicht (in Teilen) in einem Wörterbuch vorkommen.

Der Begriff „Wörterbuch“ ist hierbei nicht eng auf ein Nachschlagewerk wie etwa den Duden anzuwenden, sondern beinhaltet alle bekannten Phrasen und Zeichenkombinationen (u.a. umgangssprachliche Verfremdungen, Abkürzungen, Akronyme, Muster auf der Tastatur), die in einem mehr oder weniger breiten Verwendungsraum bekannt sind. Illegal abgegriffene Passwortlisten werden hierbei ebenso als Wörterbuchattacke genutzt wie alle offiziell bekannten Quellen und Sprachen. Vielfach werden sogar fertig vorberechnete bzw. illegal abgegriffene Hash-Tabellen (sogenannte Rainbow-Tabellen, siehe z.B. https://de.wikipedia.org/wiki/Rainbow_Table) benutzt, was bei einem Angriff dann noch schneller zum „Erfolg“ führt als eine reine Brute-Force-Attacke.

Nun stößt man als Mensch sehr schnell an natürliche Grenzen der Merkfähigkeit. Mehrere komplexe und unstrukturierte Passwörter kann sich kaum jemand im Kopf merken. Er braucht eine Stelle, an der er seine Passwörter sicher abspeichern kann.

Eine praktikable Lösung sieht so aus, dass man eine verschlüsselte Passwortdatenbank nutzt, in der alle Passwörter und Zugangskennungen gesichert gespeichert sind. Diese Datei verwahrt man an sicherer Stelle (z.B. auf einem verschlüsselten USB-Stick offline und getrennt vom Rechner) und sichert die Passwortdatenbank mit einem sehr sicheren Masterpasswort ab. Man muss sich fortan nur noch ein Masterpasswort merken und kopiert die spezifischen Passwörter dann bei Bedarf per Copy & Paste aus der Datenbank in die Anmeldemasken der jeweiligen Systeme.

Ein gutes System ist Keypass, welches nach allgemeiner Auffassung noch nicht erfolgreich gehackt werden konnte (Quelle: http://keepass.info/).

Passwort-Tipps

- Wählen Sie möglichst lange Passwörter
- Halten Sie Passwörter grundsätzlich geheim
- Wechseln Sie die Passwörter regelmäßig
- Hinterlegen Sie die Passwörter in einem versiegelten Umschlag im Tresor
- Benutzen Sie möglichst komplizierte Passwörter aus Buchstaben (incl. Groß-Klein-Schreibung), Sonderzeichen und Zahlen
- Passwörter, die Sie z.B. aus den Anfangsbuchstaben eines Liedtextes oder eines Satzes bilden, können Sie sich leicht merken (bitte aber nicht dieses): „Hoch auf dem gelben Wagen, sitz ich beim Schwager vorn.“ liefert als Passwort „HadgW,sibSv.“

Extrem schlechte Passwörter

- Es gibt überhaupt kein Passwort
- Das vom Administrator gesetzte Default-Passwort wird beibehalten
- Das Passwort ist mit der Kennung identisch

- Das Passwort ist der Nachname oder Vorname des Benutzers
- Als Passwort wird "Passwort", "Pass" oder auch "geheim" eingegeben
- Das Passwort ist so kompliziert, dass man es sich nicht merken kann und es deshalb aufschreibt (die berühmten "Zettel unter der Tastatur bzw. am Bildschirm")

Ganz schlechte Passwörter

- Das Passwort wird auf einfache Art (Abkürzung, Buchstabenumstellung, Anhängen von Zahlen, Rückwärts schreiben) abgeleitet aus
    - der Kennung
    - Namen von Orten
    - Zeichenfolgen, die zum persönlichen Umfeld gehören wie z.B. das Geburtsdatum, die Hausnummer, Telefonnummern
    - Rechnernamen
- Worte aus dem Sprachschatz (div. Wörterbücher)
- Worte aus anderen Sprachen (ebenfalls div. Wörterbücher)
- Wörter, die häufig für Gastkennungen als Passwörter vergeben werden (guest, gast, public, common)
- bekannte Kult-Wörter wie z.B. "wizard", "spock", "merlin", "guru", "gandalf", ...
- Name der Institution, die den Rechnerzugang zur Verfügung stellt, z.B. „BMW" oder Name des Arbeitsplatzes: „Sekretariat“
- Firmenlogo am Monitor, Tastatur, PC

Schlechte Passwörter

- Vermeintlich unsinnige Kombinationen aus Buchstaben und Zahlen, die in Wirklichkeit jedoch einfach zu merkende oder bequem nebeneinander liegende Tastaturkombinationen sind wie "abc123", "1234qwer", "qwertz", "qwerty", "abc:123"

- Das Passwort wird der Sache oder dem Benutzernamen angepasst: für den E-Mail-Account also "E-Mail", für das Haustierforum = "Haustier"
- Benutzername = "Adam", Passwort = "Eva" usw. - bequem zu merken, aber sehr leicht zu erraten
- **bekannte** Eselsbrücken
    - GDaEhFis = Tonleiter: G-Dur (Geh Du alter Esel hole Fische)
    - EaDGhe = Gitarrensaiten (Eine alte Deutsche Gitarre hält ewig)
- Anfangsbuchstaben von **bekannten** Sprichwörtern, Liedern etc. wie z.B.
    - AmEsadS = Alle meine Entchen schwimmen auf dem See
    - WrssdNuW = Wer reitet so spät durch Nacht und Wind

Gute Passwörter

- sind länger als 9 Zeichen (besser 10 und mehr)
- enthalten mindestens zwei Ziffern oder Sonderzeichen, diese stehen nach Möglichkeit nicht nur am Anfang und/oder Ende
- kann man sich leicht merken
- kann man schnell eintippen (das Passwort ist durch Über-die-Schulter-Schauen nicht leicht erkennbar)
- enthalten keine (erkennbare) Systematik, d.h. erscheint wie eine zufällig erzeugte Zeichenfolge
- sind kein Wort einer bekannten Sprache
- sind nur dem Inhaber der Kennung bekannt

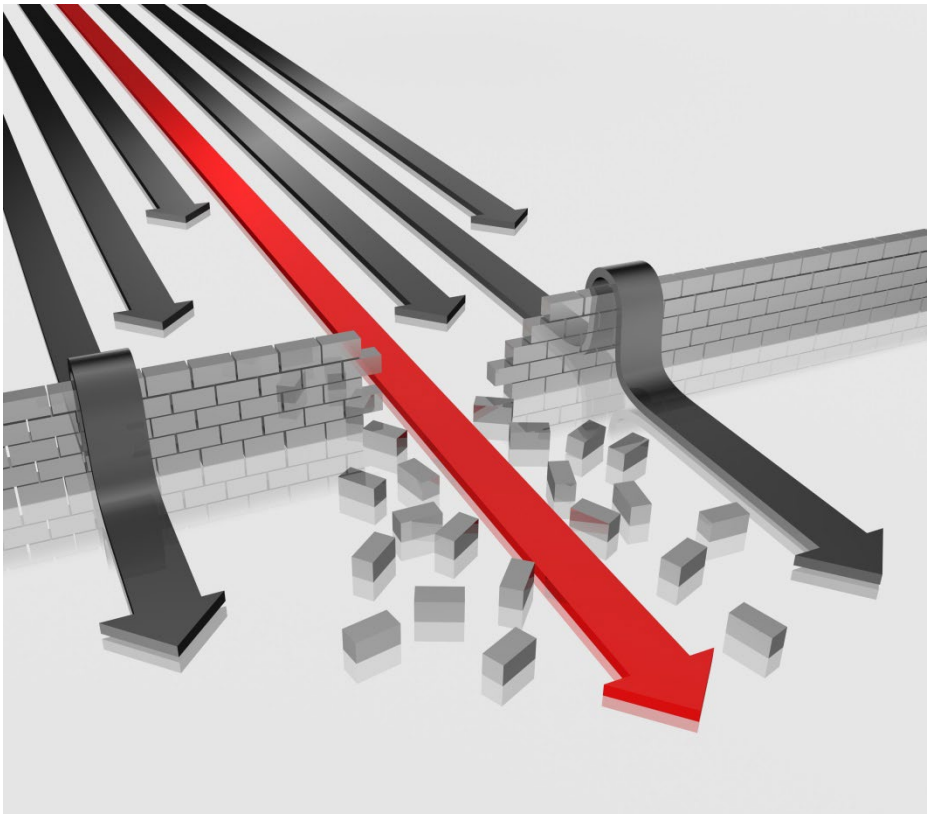
Allgemein gilt: Für verschiedene Kennungen sollte man verschiedene Passwörter wählen.

Angriffe von innen – Social Engineering

Die Bedrohungs-Szenarien Datenausspähung, -manipulation und -zerstörung entspringen hierbei nicht immer dem „bösen“ Internet, 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.

Deaktivieren (nicht Löschen) Sie daher unverzüglich sämtliche Zugangsberechtigungen eines ausscheidenden Mitarbeiters (mit Beginn der Freistellung) für Ihr internes LAN und externe Web-Services (incl. E-Mail Zugänge etc. per Smartphone und Web-Access) und ändern Sie alle Passwörter und Zugangskennungen, die der ehemalige Mitarbeiter kennen könnte. Denn auch wenn er oder sie nicht mehr im Unternehmen (vor Ort) ist, gibt es ggf. immer noch offene Zugänge zu den E-Mail-Konten und Portalen der Firma. Und wenn dem Ex-Mitarbeiter Kennungen von Kollegen bekannt sind (z.B. weil alle Mitarbeiter dasselbe Passwort benutzen), dann kann er womöglich noch jahrelang unbemerkt auf die E-Mails seiner Kollegen zugreifen. Böse, wenn er dann bei einem Konkurrenzunternehmen Ihre mühsam akquirierten Aufträge abgreift…

Angriffe von außen



Die Bedrohungs-Szenarien, die von außen an ein EDV-System herangetragen werden, sind sicherlich vielfältiger und weiter verbreitet. Gilt ein IT-System ohne Kommunikationsschnittstellen nach außen (Online, Datenträgeraustausch etc.) per se als sicher (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 Trojaner[6], um sie dann gezielt nach verwertbarem Material zu durchforsten.

Direkte Angriffe

So ist der einzelne Rechner oder ein Firmennetzwerk oft aus dem Internet gar nicht ohne Kenntnisse 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 Providern 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 verseuchte E-Mails oder Webseiten sogenannte Würmer und Trojaner in die Systeme einzuschleusen, die dann, einmal im Wirts-Systems eingenistet, 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.

---

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

Phishing

Eine andere, mittlerweile sehr verbreitete Form der Datenausspähung ist das sogenannte „Phishing“. Dieses Kunstwort beschreibt das „Passwort Fishing“, d.h. das Fischen nach Passwörtern beispielsweise im E-Mail- und Online-Verkehr durch Umleiten von Benutzereingaben auf entsprechend präparierte Web-Seiten.

Hierbei wird z.B. eine offiziell aussehende E-Mail 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 über die in der E-Mail enthaltenen Hyperlinks erfolgt, landet dann jedoch nicht bei dem richtigen Online-System Ebay®, sondern wird von einem Hacker-System abgefangen.

Man-in-the-middle-Attacken

Die „Perfektion“ solcher Angriffe sind 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 Bankinstitut 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 weiterzureichen, um ihn in Sicherheit zu wiegen. Bei einer nachfolgenden Transaktion (Online-Überweisung) leitet er jedoch die Eingaben nicht an die Bank weiter, sondern simuliert die Antworten der Bank lediglich.

Nachfolgend überweist er mit Hilfe der mitgeschriebenen Passwörter und TAN[7]-Nummern einen Geldbetrag auf ein von ihm kontrolliertes Konto. Der Nachweis einer solchen Manipulation ist dann nicht einfach und der Anwender wird möglicherweise beweispflichtig.

Sichere Kommunikation

Um dies zu vermeiden, bedient man sich daher sinnvollerweise gerade bei kritischen Übertragungen entsprechend gesicherter Verfahren wie beispielsweise der SSL-Kommunikation oder Online-Banking-Standards wie z.B. dem HBCI-Verfahren[8]. 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. Starmoney®, SFirm® usw. Sicherheitsvorteile, da hier von den Programmen gesteuerte und überwachte Übertragungen stattfinden und keine unsichere Kommunikation über Web-Browser durch den Benutzer initiiert wird.

Zur Vertiefung der Themen Phishing und Man-in-the-middle-Attacken sei dem Leser die 1. Ausgabe der Reihe DigiFor Inside „Social Engineering und Phishing am Beispiel von Facebook & PayPal“ empfohlen, die sich eingehend mit diesem Angriffsszenario beschäftigt.

---

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

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

Fernwartung

Besonderes 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 ob man direkt davor sitzt. Was im Problem- und Fehlerfall ein Segen sein kann und schnelle Hilfe ermöglicht, kann im Missbrauchsfall katastrophal sein. Ein gehackter Fernzugang kann so z.B. 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 gekommenen WLAN's. 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 Räume des Betreibers 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 bzw. nicht ausreichend geschützt betrieben werden, begründet durch die meist 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.

Ist erst einmal ein Angreifer in das Netzwerk eingedrungen und der Transport der Datenpakete unverschlüsselt, dann hat er umfangreiche Möglichkeiten zum Mitlesen und Verfälschen der (Ihrer) Daten. Mit einfach zu bedienenden und frei erhältlichen Toolkits (wie z.B. ettercap) „verbiegt“ er die DNS-Adressen im WLAN/LAN und leitet fortan jeglichen Traffic beispielsweise statt an Facebook, PayPal oder der (Ihrer) Hausbank auf seinen Angreifer-PC um. Das fatale daran: Ohne konkreten Verdacht, dass ein solches ARP- bzw. DNS-Spoofing im Gange ist, merkt selbst ein Fachmann nicht unbedingt oder sofort, dass die Daten mitgelesen werden.

Sichern Sie Ihr WLAN daher unbedingt mindestens mittels WPA2 ab und halten Sie den sogenannten Preshared-Key geheim! Am besten: Sie lassen das von einem Fachmann einrichten und prüfen! Wie ein Angriff auf ein WLAN funktioniert und wie man sich schützen kann, finden Sie in dem bereits erwähnten Fachartikel DigiFor Inside Ausgabe 1 „Social Engineering und Phishing am Beispiel von Facebook & PayPal“.

Einschleusen von Schadcode

Eine weitere Gefahr für Ihre Daten besteht durch Einschleusen von Schadcode durch sogenannte Bufferoverflows oder Cross-Site-Scripting. Dieses Thema wird in Ausgabe 2 der DigiFor-Inside-Reihe ausführlich behandelt:

„Bufferoverflows – Wie man Programmierfehler zum Einschleusen von Schad-Code nutzen kann“

Computer Forensik

Intrusion Detection

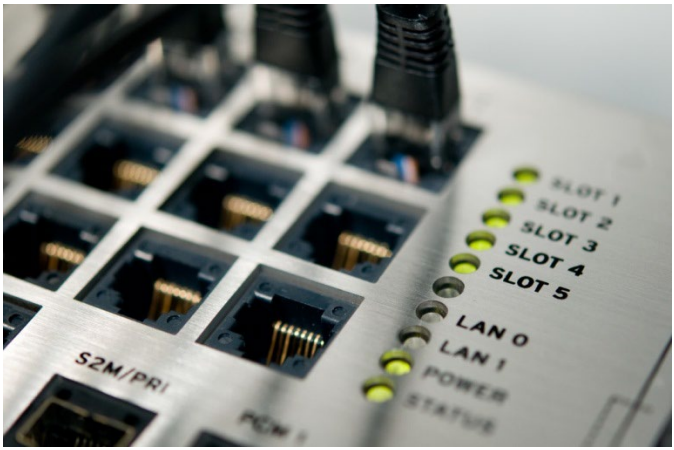
Da kein System der Welt als 100% sicher vor Einbrüchen und Manipulationen angesehen und faktisch jede noch so ausgeklügelte Sicherheitsbarriere mit entsprechendem Aufwand umgangen werden kann, kommt der Feststellung, dass es einen konkreten Angriff auf die EDV gibt oder gab und nachfolgend der entsprechenden 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 Rückgrat 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[9]).

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 aufwendig. 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.

[9] Incident = (sicherheitsrelevanter) Vorfall; Response = Reaktion, Antwort

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.



Regeln für den Fall der Fälle

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 Herunterfahren eines Systems werden jedoch 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 vorliegt, so sind unbedingt in einem ersten Schritt die Ermittlungsbehörden einzuschalten. Die Polizei-Präsidien unterhalten zu diesem Zweck entsprechend mit Fachleuten ausgestattete Kommissariate, die die Ermittlungen 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.

Schutzmechanismen

„Gefahr erkannt – Gefahr gebannt“ so beschreibt der Volksmund den ersten Schritt zu mehr Sicherheit. Ist erst einmal eine gewisse Sensibilisierung für die Themen Datensicherung, Datensicherheit und 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 (Sicherheits-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 E-Mail.

8. Verlangen Sie für rechtssichere 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 E-Mail 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.

Wenn Sie Beratung in diesem Bereich benötigen oder einen konkreten sicherheits-relevanten Vorfall haben, dann können Sie sich gerne an den Autor Dipl.-Ing Thomas Käfer wenden.

Fazit

Gelangen durch direkte oder indirekte Hacker-Attacken oder fahrlässigen Umgang der Betreiber personenbezogene oder andere unternehmenswichtige Daten in die falschen Hände oder an die Öffentlichkeit, ist der Schaden groß.

Es drohen Image- und Vertrauensverlust und ggf. hohe Schadensersatzforderungen der Betroffenen. In der Folge werden unter Umständen aufwendige Audits durch die Überwachungsbehörden nötig und es erwachsen schnell zivil- und strafrechtliche Konsequenzen gegen die Betreiber, wenn personenbezogene Daten unsachgemäß, grob fahrlässig oder unzureichend geschützt gespeichert und übertragen wurden.

Mit so einem Thema möchten Sie sich nicht in der Tagespresse oder gar in den Abendnachrichten wiederfinden!

Lesen Sie in der nächsten Ausgabe von DigiFor Inside „Die Tools der Hacker – Backtrack, Kali Linux & Co“

Bezug und weitere Informationen und Artikel siehe:
http://www.KaeferLive.de/digifor-inside

Ihr

Thomas Käfer

P.S. Und wenn Sie ein echtes Sicherheitsproblem haben oder dieses für die Zukunft vermeiden möchten, dann kontaktieren Sie uns. Wir kümmern uns darum: Tel. 02405/479490 oder E-Mail service@KaeferLive.de.

Beachten Sie auch unsere speziellen Security-Angebote, wie z.B. die Aktion „Unser Netz soll sauberer werden“ in unserem Online-Shop:

http://shop.kaeferlive.de/product_info.php?info=p51_aktionspaket--unser-netz-soll-sauberer-werden.html

Schlagwörter