

DS-G

Autor: Peter Wies, Konrad Stulle

Inhaltliches Lektorat: Wolfgang J. Weber

1. Ausgabe vom 21. März 2006

© by HERDT-Verlag für Bildungsmedien GmbH,
Bodenheim

Internet: www.herdt4you.de/at
www.herdt4business.de/at
www.herdt4vhs.de/at

Alle Rechte vorbehalten. Kein Teil des Werkes darf in irgendeiner Form (Druck, Fotokopie, Microfilm oder einem anderen Verfahren) ohne schriftliche Genehmigung des Herausgebers reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

Diese Unterlage wurde mit großer Sorgfalt erstellt und geprüft. Trotzdem können Fehler nicht vollkommen ausgeschlossen werden. Verlag, Herausgeber und Autoren können für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen.

Die Bildungsmedien des HERDT-Verlags enthalten Links bzw. Verweise auf Internetseiten anderer Anbieter. Auf Inhalt und Gestaltung dieser Angebote hat der HERDT-Verlag keinerlei Einfluss. Hierfür sind alleine die jeweiligen Anbieter verantwortlich.

Datensicherheit

Grundkurs

DS-G

1 Über diese Unterlage	4	7 Sicherheitseinstellungen für das Internet.....	60
1.1 Was Sie wissen sollten	4	7.1 Internet Explorer sicher einstellen	60
1.2 Nützliche Techniken.....	5	7.2 Sicherheitszonen einstellen	61
2 Datensicherheit und Datenschutz.....	8	7.3 Umgang mit Cookies	65
2.1 Was versteht man unter Datensicherheit?	8	7.4 Persönliche Informationen verwalten	66
2.2 Standards im Bereich Datensicherheit	10	7.5 Spezielle Zugriffsbeschränkungen einrichten	67
2.3 Sicherheitsrichtlinie (Security Policy)	12	7.6 Sicherer Datenaustausch im Internet.....	69
2.4 Die Problematik des Datenschutzes	13	7.7 Sicherheitszertifikate einsetzen	70
2.5 Datenschutzgesetze in Europa und Deutschland.....	14	7.8 Das Webseiten-Zertifikat einsetzen	70
3 Sicherheitsprobleme durch Mitarbeiter.....	16	7.9 Schnellübersicht	71
3.1 Mangelnde Kompetenz	16	8 PC vor Viren, Spyware und Dialern schützen	72
3.2 Ausfall/Krankheit.....	17	8.1 Antivirenprogramme verwenden	72
3.3 Spionage.....	18	8.2 Erste Schritte bei einer Vireninfektion	73
3.4 Social Engineering.....	19	8.3 AntiVir installieren.....	73
4 Gefahren durch Viren, Dialer und Spyware	22	8.4 Einstellungen für die Virensuche festlegen	74
4.1 Grundsätzliches zu Computerviren	22	8.5 Datenträger auf Viren überprüfen	75
4.2 Übersicht über Viren und andere Schadensprogramme.....	24	8.6 Auf gefundene Viren reagieren	77
4.3 Ablauf eines Angriffs	29	8.7 Dateien beim Öffnen und Schreiben auf Viren prüfen	80
4.4 Gefahr durch Dialer.....	31	8.8 Regelmäßig nach Viren suchen.....	81
4.5 Gefahr durch Spyware	33	8.9 AntiVir über das Internet updaten	82
4.6 Sicherheitsrisiken im Internet.....	35	8.10 PC vor Spyware schützen.....	83
4.7 Informationen im Internet zum Thema Datensicherheit.....	37	8.11 PC vor Dialern schützen	85
5 Sicherheitsaspekte in Netzwerken.....	38	8.12 Schnellübersicht	87
5.1 Was zeichnet ein Netzwerk aus?	38	9 Firewalls verwenden	88
5.2 Client und Server	40	9.1 Grundlagen zu Firewalls	88
5.3 Peer-to-Peer-Netzwerke	40	9.2 Die Firewall von Windows XP nutzen	89
5.4 Der Server	42	9.3 Personal Firewall verwenden.....	91
5.5 Strukturierte Netzwerke	43	9.4 ZoneAlarm installieren und starten	93
5.6 Internetzugang über DSL-Router einrichten	44	9.5 Mit ZoneAlarm arbeiten	95
6 Systemeigene Schutzmöglichkeiten vor Angriffen	46	9.6 ZoneAlarm einstellen und testen	97
6.1 Passwörter verwenden	46	9.7 Schnellübersicht	103
6.2 Tipps zum Umgang mit Passwörtern	47	10 Grundlagen zur Datenverschlüsselung....	104
6.3 Sicheres Arbeiten mit dem Computer	48	10.1 Grundlegende Informationen zur Kryptografie	104
6.4 Sicherheitseinstellungen unter Windows vornehmen.....	51	10.2 Symmetrische Verschlüsselung.....	105
6.5 Windows aktualisieren	56	10.3 Asymmetrische Verschlüsselung	106
6.6 Schnellübersicht	59	10.4 Public Key Infrastructure.....	107
		11 Daten mit PGP verschlüsseln.....	110
		11.1 PGP installieren und Schlüssel generieren....	110
		11.2 Schlüssel exportieren und importieren.....	112

11.3	Schlüssel signieren.....	115	14 Daten sichern bzw. endgültig löschen	144	
11.4	E-Mail signieren und verschlüsseln	116	14.1	Datenbestände sichern	144
11.5	Dateien endgültig und sicher löschen	118	14.2	Die Datensicherung (Backup) unter Windows XP	147
11.6	Dateien mit systemeigenen Mitteln schützen	119	14.3	Erweiterte Systemsicherung unter Windows XP	150
11.7	Schnellübersicht	121	14.4	Die manuelle Datensicherung unter Windows 2000.....	152
12 Internetbanking und E-Commerce			122		
12.1	Grundlagen des Internetbankings.....	122	14.5	Regelmäßige Datensicherung unter Windows XP	154
12.2	Voraussetzungen des Homebankings	123	14.6	Regelmäßige Datensicherung unter Windows 2000.....	156
12.3	Sicherheit des Homebankings/ Internetbankings	124	14.7	Sicherungskopie wiederherstellen.....	158
12.4	Bankgeschäfte online erledigen.....	127	14.8	Dateien unter Windows XP in komprimierten Ordnern speichern	159
12.5	Einkaufen im Internet.....	130	14.9	Dateien unter Windows 2000 in ZIP- Archiven speichern.....	161
12.6	Schnellübersicht	133	14.10	Sensible Daten endgültig löschen	164
13 Systemdateien sichern.....			134		
13.1	Startdisketten bzw. Boot-CD erstellen	134	14.11	Schnellübersicht.....	164
13.2	Registrierung sichern und wiederherstellen....	135	Anhang: So finden Sie die Inhalte zu den Lernzielen.....		
13.3	Schlüssel in der Registrierung verwalten.....	137	166		
13.4	Einstellungen von Windows XP sichern.....	141	Stichwortverzeichnis		
13.5	Schnellübersicht	143	168		

3 Sicherheitsprobleme durch Mitarbeiter

In diesem Kapitel erfahren Sie

- wie Mitarbeiter Sicherheitsprobleme verursachen können
- wie Sie diese Sicherheitslücken vermeiden können

Voraussetzungen

- ✓ Kenntnis der Betriebsabläufe innerhalb einer Firma

3.1 Mangelnde Kompetenz

Falsche Bedienung

Die Hauptursache für Sicherheitsprobleme liegt - im Gegensatz zu den vorsätzlichen Sicherheitsverletzungen - in der mangelnden Kompetenz der Mitarbeiter. Viele erhalten, wenn überhaupt, nur eine kurze Einarbeitung in die IT-Umgebung am Arbeitsplatz. Findet diese statt, so ist sie meist auf das Ziel "Erfüllung der Aufgabe" ausgerichtet, nicht aber auf die Sicherheit im Betrieb.

So ist es nicht überraschend, wenn viele Sicherheitsprobleme durch Fehlbedienung durch Benutzer entstehen. Teilweise wird dies auch durch unergonomische Software mit verwirrenden Dialogen und umständlicher Bedienung gefördert. Zu den wichtigsten Problemen gehören:

- Versehentliches Löschen von Dateien
- Versehentliches Senden von sensiblen Daten an Unberechtigte
- Falsche Änderungen an Datenbeständen

Fehlerhafte Konfiguration, veraltete Software

Auch auf der administrativen Seite überwiegt der menschliche Anteil der Fehlerursachen und Sicherheitsrisiken. Die unzureichende Konfiguration von Software oder eine Installation ohne weitere Wartung und Konfiguration lässt teilweise viele Sicherheitsprobleme unberücksichtigt. Durch vermehrt eingesetztes Plug & Play in Hard- sowie Software ist es für den Administrator vielfach einfacher geworden, eine lauffähige Installation zu erhalten, ohne sich konkret mit dem neuen System selbst auseinander zu setzen und die daraus resultierenden Implikationen für die IT-Sicherheit zu bedenken.

Meist haben die Administratoren auch nicht viele Alternativen, da dem Thema Sicherheit zwar im Marketing und auf der Managementebene viel Bedeutung beigemessen wird, aber im operativen Geschäft keine bzw. nur wenig Zeit und Ressourcen für Sicherheitsprozesse aufgewandt werden. So ist der Administrator auf Grund seiner vielfältigen Aufgaben z. B. gezwungen, einen Webserver nur zum Laufen zu bekommen, weil er sich schon um die nächste Aufgabe kümmern muss.

Dass dies in vielen Unternehmen gängige Praxis ist, zeigen beispielsweise die Code-Red- und Nimda-Epidemien im Jahr 2001. Diese beiden Viren nutzten eine Sicherheitslücke im Microsoft Internet Explorer oder Internet Information Server aus, die schon im Frühjahr bekannt geworden war und mit entsprechenden Patches geschlossen werden konnte. Nichtsdestotrotz trat Ende Juli/Anfang August eine weltweite Code-Red-Epidemie auf, gefolgt von einer Nimda-Epidemie ab Mitte September 2001. Auch Sommer/Herbst 2002 waren noch regelmäßig kleinere Ausbrüche von Nimda-Epidemien in Deutschland zu beobachten.

Daran lassen sich folgende Sachverhalte ablesen:

- Viele Internet Information Services/Internet-Explorer-Installationen werden direkt von der ersten Installationsquelle durchgeführt, ohne jemals einen Patch einzuspielen.
- Viele Systeme bleiben auch nach ihrer Erstinstallation monatelang ungepatcht.

- ☑ Auch nach einer flächendeckenden Epidemie, die durch eine bekannte Sicherheitslücke ausgelöst wurde, und entsprechender Präsenz in den Medien wurden viele Systeme **immer noch nicht gepatcht**, was die Ausbreitung von Nimda im September extrem begünstigte.
- ☑ Viele Windows Server, die die Internet Information Services gar nicht benötigen, betreiben diese anscheinend trotzdem, da sie bei einer Standardinstallation mitinstalliert wurden und vom Administrator in der Folge weder deaktiviert noch gewartet oder überprüft werden.

Unwissenheit bei Vorschriften und Arbeitsvorgängen

Vielerorts wissen Mitarbeiter nicht um die speziellen Vorschriften, die für die IT-Sicherheit an ihrem Arbeitsplatz gelten. Eine noch so gründlich erarbeitete Sicherheits-Policy kann vom Mitarbeiter nicht berücksichtigt werden, wenn dieser bei seiner Einarbeitung niemals von ihrer Existenz unterrichtet worden ist. Besonders verheerend ist es, wenn z. B. der Posten eines Datenschutzbeauftragten oder IT-Sicherheitsbeauftragten intern einem beliebigen Mitarbeiter zugeteilt wird, der nicht über die notwendige Fachkompetenz zur Erfüllung dieser Aufgaben verfügt. Diese Person kann selbst bei bestem Willen aus dem Stand keine vernünftige Policy entwerfen.

Solange der einzige Mitarbeiter, dem die Policy bekannt ist, der IT-Sicherheitsverantwortliche ist, der sie erstellt hat, kann die Policy auch nicht wirksam sein. Deswegen ist eine Einführung in Vorschriften und Arbeitsvorgänge ein unerlässlicher Bestandteil der Einarbeitung.

Schulen Sie nicht nur das IT-Personal und die IT-Sicherheits-Mitarbeiter, sondern die gesamte Belegschaft. Die Wahrscheinlichkeit, dass ein erfahrener Administrator ein unverlangt von Unbekannten zugesendetes Attachment öffnet, ist deutlich geringer, als dass ein Mitarbeiter einer Nicht-IT-Abteilung aus Neugier ein derartiges Attachment ausführt.

Da in den meisten Unternehmen Mitarbeiter in Nicht-IT-Abteilungen den Großteil des Personals bilden, besteht hier die größte Angriffsfläche.

Das gesamte Personal sollte deswegen für die verschiedenen Erscheinungsformen von Sicherheitsproblemen sensibilisiert werden.

3.2 Ausfall/Krankheit

Wer hat das Passwort?

Die Person mit den höchsten Befugnissen in einem Netzwerk ist üblicherweise der Netz- oder Systemadministrator. Unabhängig davon, ob die Verwaltungsaufgaben in kleineren Firmen nur von einer Person ausgeübt werden oder in großen Netzwerken auf viele Administratoren mit genau definierten Aufgabenbereichen verteilt werden, besitzen alle Administratoren erweiterte Zugriffsrechte, um ihren Aufgaben nachkommen zu können.

Administratoren sind also Informationsträger besonderer Art. Nicht nur, dass sie im Besitz der höher berechtigten Accounts sind, sie wissen auch um Aufbau und Organisation der von ihnen verwalteten Rechnernetzwerke.

In vielen Firmen sind für geplante Abwesenheitszeiten dieser Mitarbeiter schon Regelungen in Kraft, die zum Beispiel vor dem Urlaubsantritt eines Administrators eine Übergabe von Informationen und Berechtigungen an die Vertretung vorsehen. Kommt es aber zu einem unvorhergesehenen Ausfall eines Mitarbeiters, z. B. durch einen Unfall, eine schwere Krankheit oder Tod, so kann dies gravierende Konsequenzen für die EDV eines Unternehmens haben, wenn dieser Mitarbeiter als Einziger für die Netzwerkverwaltung oder einen Teilbereich davon zuständig war.

Auch die unerwartete Kündigung eines Mitarbeiters kann derartige Konsequenzen nach sich ziehen. Möglicherweise wird zwar das Administratorpasswort übergeben, aber während eines kurzen Übergabegesprächs wird es kaum möglich sein, alle denkbaren Besonderheiten der Organisations- und Verwaltungsaspekte des Netzwerks zu besprechen, über die nur der scheidende Administrator Bescheid wusste. Dies kann auch lange nach dem Ausscheiden des alten Administrators noch zu unangenehmen Überraschungen für seinen Nachfolger führen.

Den Notfall einplanen

Es empfiehlt sich also, bei der Planung von Vertretungsregelungen auch unvorhergesehene Fälle zu berücksichtigen, um die Fortführung der administrativen Tätigkeiten zu gewährleisten. Damit derartige Regelungen greifen können, sollten folgende Bedingungen erfüllt sein:

- Der Stand von Projekten, Konfigurationen und Verfahrensweisen muss jederzeit ausreichend (schriftlich) dokumentiert sein.
- Die Benennung einer Vertretung alleine reicht nicht aus, um eine Fortführung der geforderten Tätigkeiten im Notfall garantieren zu können. Es ist zu prüfen, ob und wie die Vertretung geschult werden muss, damit sie auch in der Lage ist, die gestellten Aufgaben bei Bedarf zu erfüllen. Wenn sich bei einer derartigen Überprüfung herausstellt, dass auf Grund des geforderten Spezialwissens kurzfristig keine Ersatzkraft eingesetzt werden kann, ist es besonders wichtig, diese Kräfte langfristig zu schulen.
- Es muss genau definiert sein, welche Aufgaben im Notfall auf welche Vertreter aufgeteilt werden.
- Der Vertreter darf die erforderlichen Berechtigungen nur im Notfall erhalten (also keine Admin-Rechte auf Vorrat).
- Wenn es nicht möglich ist, für Personen einen kompetenten Vertreter zu benennen oder zu schulen, sollte der Einsatz einer externen Vertretung eingeplant werden.

Besonders kritisch ist die Situation, wenn Sie bei der Analyse des Ist-Zustands bei Personalaufgaben an einen "Single-Point-of-Knowledge" gelangen. Besitzt eine einzelne Person das alleinige Spezialwissen, um eine bestimmte IT-Aufgabe wahrnehmen zu können, so sollten Sie mit besonderer Sorgfalt für deren Ausfall Vertreter schulen oder externe Fachkräfte auswählen.

3.3 Spionage

Datenmitnahme

Mitarbeiter, die berechtigt sind, Informationen zu lesen, können diese Berechtigung auch nutzen, um eine Kopie dieser Daten anzufertigen. Spätestens dann, wenn die Notwendigkeit nicht mehr vorhanden ist, dass ein Benutzer auf bestimmte sensible Daten zugreifen können muss, sollte ihm also die entsprechende Berechtigung wieder entzogen werden.

Da nur schwer verhindert werden kann, dass während der befugten Arbeit mit sensiblen Daten bereits Kopien angefertigt werden, sollten in Bereichen mit hohem Sicherheitsanspruch Überlegungen angestellt werden, wie der Transport von Daten aus dem geschützten Bereich heraus verhindert werden kann. Besonders die weite Verbreitung von USB-Anschlüssen an modernen PCs und die hohe Verfügbarkeit von entsprechenden USB-Memory-Sticks stellen mangels ausreichender ins Betriebssystem integrierter Kontrollmethoden derzeit ein Problem dar.

Folgende Überlegungen sollten hier angestellt werden:

- Sind in den PCs Diskettenlaufwerke/USB-Ports installiert?
- Gibt es eine Möglichkeit für Benutzer, externe Laufwerke (USB Flash Memory-Sticks, CD-Brenner, ZIP, Wechselplatten etc.) anzuschließen, um Daten zu kopieren?
- Besteht vom geschützten PC aus die Möglichkeit eines Internetzugangs?
- Wenn der Internetzugang nötig ist: Welche Programme sind zugelassen bzw. unabdingbar notwendig?

Erpressung/Manipulation

Statistiken über Schadensfälle im IT-Bereich weisen darauf hin, dass die Mehrheit der Fälle von den eigenen Mitarbeitern verursacht wurden und nur ein geringer Anteil von unternehmensfremden Personen.

Mitarbeiter, die einen Groll gegen das Unternehmen hegen, könnten erhebliche Schäden verursachen, indem sie z. B. die entwendeten Kundendaten oder Forschungsergebnisse veröffentlichen. Verärgerte Mitarbeiter (zu wenig Gehalt, Kündigung o. Ä.) können mit solchen Aktionen drohen, da sie viel leichter als Hacker direkten Zugriff auf unternehmenskritische Daten haben, die sie manipulieren oder löschen können.

Online Social Engineering

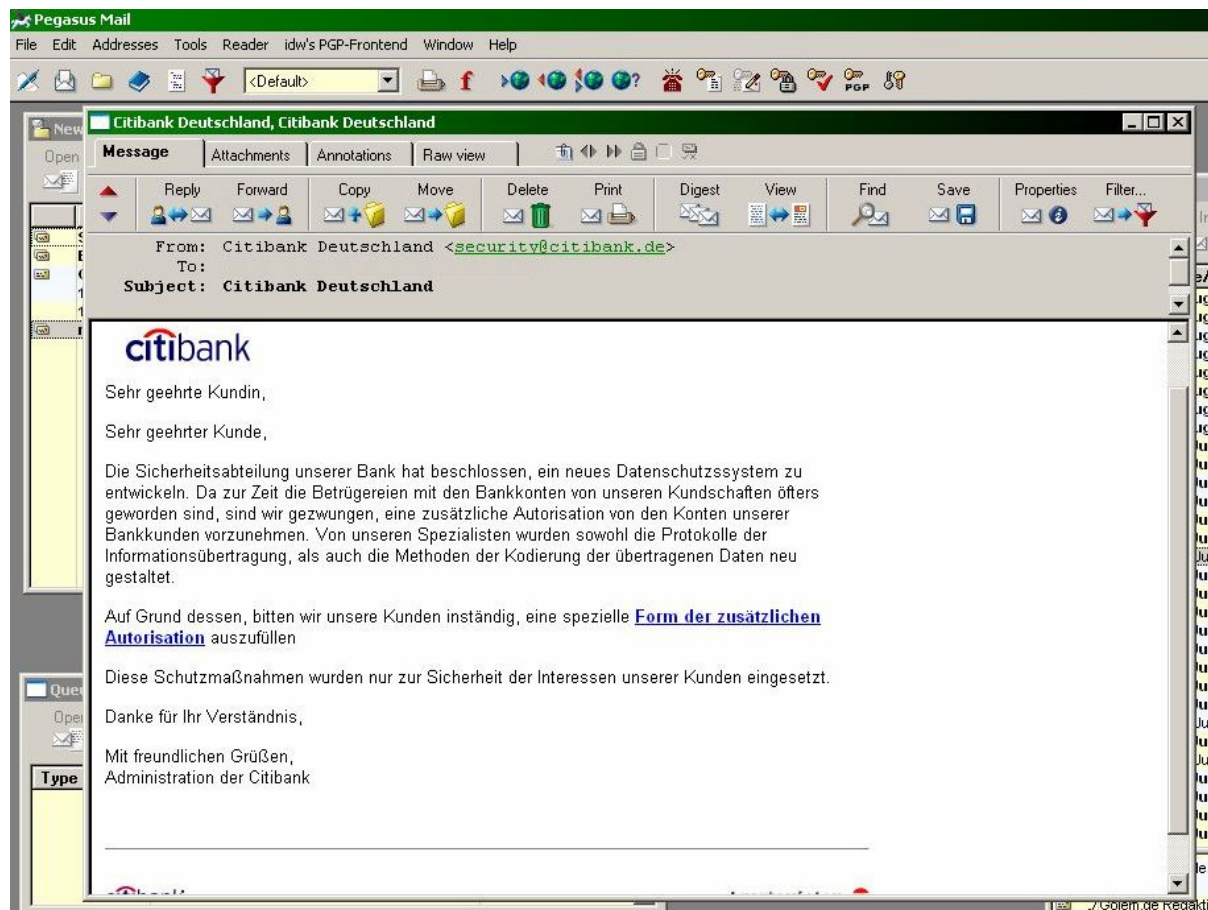
Online Social Engineering benutzt das Internet selbst, um neue Informationen zu gewinnen:

"Sie könnten gewinnen!", heißt es beispielsweise in einer E-Mail an einen Mitarbeiter. Um an dem Gewinnspiel teilzunehmen, muss er nur schnell einen Fragebogen ausfüllen und ein paar Details zu seinem Arbeitsplatz erläutern o. Ä. Viele Menschen denken bei der Aussicht auf einen Gewinn nicht an den Wert der Informationen, die sie in ein Formular unbekanntem Ursprungs eingeben.

Denkbar wäre auch, den Mitarbeiter einen Account für einen kostenlosen Internetdienst anlegen zu lassen: "Sichern Sie jetzt 100 MB kostenlosen Webspace", "gratis Antivirus-Download" etc. Sobald der Account angelegt wurde, kann der Hacker das eingegebene Passwort versuchsweise bei anderen Accounts desselben Mitarbeiters benutzen. Da es sehr häufig vorkommt, dass Benutzer aus reiner Gewohnheit für verschiedene Accounts dasselbe Passwort verwenden, ist diese Methode, in den Besitz von Passwörtern zu kommen, relativ erfolgreich.

Phishing

Die neueste Variante der Social-Engineering-Angriffe ist das so genannte Phishing (engl. Kunstwort aus password und fishing: Passwortfischen). Bei dieser Art des Internetbetrugs werden zuerst massenhaft Mails verschickt, die vorgeben, von einer Bank, von Online-Zahlungsdiensten oder Auktionshäusern wie Paypal oder eBay zu sein. Diese Mails gleichen in ihrem Erscheinungsbild den Mails der Originale.



Eine Phishing-Mail

In den Mails wird üblicherweise ein Link angegeben, der mit diversen Techniken verschleiert wurde. Der Link führt nicht auf die Original-Website, sondern auf eine gefälschte Webseite, die sich gegebenenfalls nur schwer von der Original-Website unterscheiden lässt.



Beispielsweise können in der URL der gefälschten Webseite Unicode-Zeichen (z. B. kyrillische Zeichen) enthalten sein, die wie lateinische Schriftzeichen aussehen. Durch die Verwendung dieser Zeichen unterscheidet sich die Adresse von der Original-Adresse, ohne dass der Unterschied in der Adresszeile des Browsers zu erkennen ist.

