

IT Sicherheit für Unternehmen



Alltägliche Meldungen zum Thema Sicherheit

Firmen-E-Mail-Adressen begehrtes Ziel von Hackern

November 27, 2007 by Web Internet

Firmen-E-Mail-Adressen begehrtes Ziel von Hackern

Hamburg, 27.11.2007 - Firmenmitarbeiter
Herausgabe der eigenen Geschäfts-E-Mail-
Missbrauch von Firmenadressen zu Spam
Damit ist diese Methode des Angriffs auf F
Abteilungen investieren inzwischen massi
E-Mails sind zu einem der beliebtesten

Wirtschaftsprüfer beging peinliche Anfängerfehler

Bei PWC beworben, Daten von Hackern
gestohlen

von Thomas Knauer

E-Commerce / 06.07.2008 / 11:10

Trackback Versenden

Fast 4 Millionen Opfer von Computer-Kriminalität

Jeder Zehnte verwendet kein Sicherheitsprogram

on A-Z

ATION

ATION

ATION

ATION

ATION

ATION

ATION

ATION

ATION

ATION

ATION

ATION

ATION

ATION

ATION

ATION

ATION

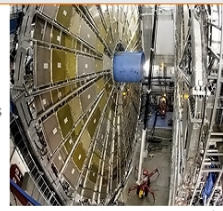
ATION

ATION

Hacker knacken offenbar Teilchenbeschleuniger

Presse: Computerfachleute als
Schüler bezeichnet

Ausgerechnet die World-Wide-Web-
Erfinder sind Opfer von Hackern
geworden: Als am CERN der neue
Teilchenbeschleuniger LHC in Betrieb
ging, drangen laut britischen Medien
Unbekannte in das Computersystem
ein - anscheinend mit rein
pädagogischem Motiv.



Am Mittwoch ging der Teilchenbeschleuniger
an den Start.

Was ist Informations- und IT-Sicherheit?

Schutzmaßnahmen

- Physikalisch Sicherheit von Personen, Gebäuden und technischer Infrastruktur
- Schäden durch Naturkatastrophen

IT-Sicherheit

- Maßnahmen zum Schutz von Daten, Applikationen, Systemen und Netzwerken

Informationssicherheit

- Alle Faktoren, die die Sicherheit von Informationen beeinflussen
- Berücksichtigt den gesamten Lebenszyklus der Information (Erstellung, Ablage, Verteilung, Modifizierung, Entsorgung)
- Die Erscheinungsform der Information ist dabei irrelevant (Papier, elektronische Daten, gesprochenes Wort...)

3

Grundlagen der Informations- und IT-Sicherheit

1. Vertraulichkeit

Hält Informationen geheim und schützt diese vor unautorisierter Einsichtnahme

2. Integrität

Schützt Daten vor unbeabsichtigter Veränderung oder bewußter Verfälschung

3. Verfügbarkeit

Stellt sicher, dass Informationen, Daten, Appl., Dienste, Systeme und Netzwerke verfügbar sind, wenn Geschäftsprozesse dies erfordern

Informations- und IT-Sicherheit

Nachweisbarkeit

Authentizität

Autorisierung

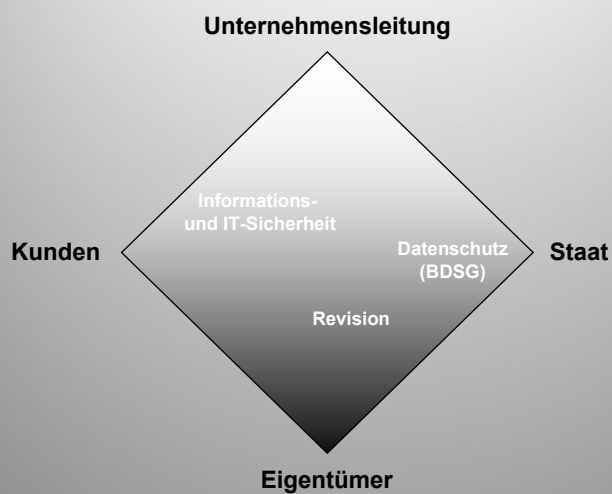
4

Zusammenwirken mit den Bereichen Datenschutz und IDW

Regelungs- bereich	Informations- und IT-Sicherheit	Datenschutz	IDW
Grundla- gen	Gesetzliche Vorgaben und themenspezifische Empfehlungen von z.T. staatlichen Organen - KonTraG - ISO 17799 - BSI - ISO 7799	Gesetzliche Vorgaben: - BDSG	Gesetzliche Vorgaben und wirtschaftliche Vorgaben der Unternehmensleitung: - HGB, AO - Grundsätze ordnungsmäßiger Speicherbuchführung (GoBS) - Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)
Inhalte	- Schutz vertraulicher und unternehmensbezogener Daten unabhängig vom Medium - Management der identifizierten, operativen Risiken	Schutz personenbezo-gener Daten vor unbefugtem Zugriff	- Abläufe und Prozesse müssen den von der Unternehmensleitung und den vorgesetzten Stellen vorgegebenen Richtlinien entsprechen. - Unwirtschaftliche Vorgänge verursachen nicht notwendige Kosten und müssen eliminiert bzw. verbessert werden.

5

Wer macht die Vorgaben?



6

Ziele von Informations- und IT-Sicherheit

- Einheitliches, angemessenes Sicherheitsniveau für alle Kunden und Anwendungen
 - von **Daten** der Kunden und der Mitarbeiter
 - der **Reputation** des Unternehmens
 - der **physikalischen** und **finanziellen Ressourcen**.

Beispiele für die Verletzung der Informationssicherheit

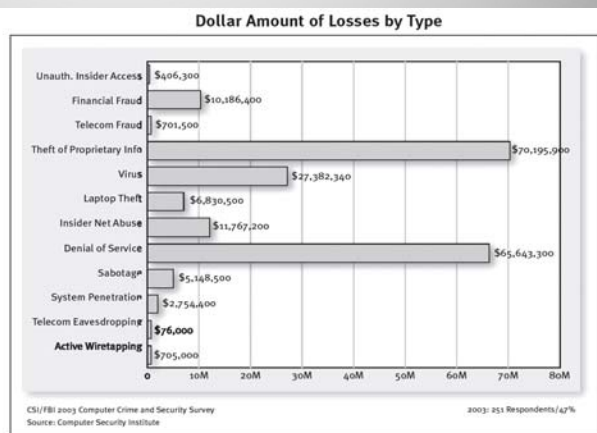
- Unautorisierte Veränderung von Informationen
- Unautorisierter Zugriff auf Informationssysteme
- Ausfall von Informationsservern durch Schadsoftware
- Verfälschung von e-Mails oder Unterschriften
- Abhören oder Aufzeichnen des Netzwerkverkehrs (z.B. e-Mails)

7

Mehrwert von Informations- und IT-Sicherheit generell

Zahlenbeispiele: CSI/FBI Computer Crime and Security Survey

- Von 530 befragten Unternehmen haben
 - 21% über Schäden durch Informationsdiebstahl und
 - 42% über Denial of Service Attacken berichtet.
- Die durchschnittliche Schadenhöhe betrug
 - **Über 1 Mio\$** für Informationsdiebstahl und
 - **600 k\$** durch DoS Attacken



8

Mehrwert von Informations- und IT-Sicherheit für die Unternehmen

- Erfüllung der vertraglichen Anforderungen (z.B. aus SLAs)
- Erfüllung der gesetzlichen Anforderungen (z.B. BDSG, KonTraG)
- Sicherheit wird nachweislich wirtschaftlich gestaltet
 - Nachweislich: auditierbar, reversionssicher, zertifizierbar
 - Wirtschaftlich: Erfolgskontrolle, Kennzahlen, bezahlbar
- Informationen und Systeme sind klassifiziert



Auswirkungen/Mehrwert für Mitarbeiter

- Definierte und verbindliche Regelungen und Vorgaben im Bereich Informations- und IT-Sicherheit liegen vor
- Klare Konsequenzen bei Nichteinhaltung
 - Kriterien: Fahrlässigkeit (Person) und Auswirkungen (Schaden)
 - Mittel: Gespräch, Weisung, Abmahnung, Kündigung
 - Eskalation gemäß bestehenden Regelungen und Prozessen (Führungskraft / Personalbereich / Betriebsrat)

Mehrwert für Mitarbeiter:

- Klarheit über „erlaubte“ und „nicht erlaubte“ Vorgehens- und Verhaltensweisen
- Schutz der eigenen Daten (Privatsphäre)
- Sicherheit des Unternehmen bedeutet auch **Sicherheit des Arbeitsplatzes**



Was kann ich als Unternehmer/ Mitarbeiter konkret tun?

11

Maßnahmen für die Mitarbeiter

Grundlage: Sicherheitsstrategie

„Sicherheit geht alle an“. Alle Nutzer sind verpflichtet, die Einhaltung der Sicherheits-Regelungen zu unterstützen und für sich selbst sicherzustellen

- Alle Nutzer werden hinsichtlich **geltender Gesetze** und dem **gleichkommender Vorschriften** geschult und zu ihrer Einhaltung verpflichtet.
- Alle Nutzer werden geschult, um ausreichende Kenntnis von den **Sicherheitsregelungen** zu erlangen.

12

Aufgaben und Pflichten als Mitarbeiter

Grundlage: Sicherheitsstrategie

- Für die Mitarbeiter besteht die Verpflichtung, sich nötigenfalls ausreichende Kenntnis zu den sicherheitsrelevanten Themen selbst zu verschaffen.
- Die Mitarbeiter sind gehalten, durch verantwortungs-bewusstes Handeln an der Umsetzung sowie aktiv an der kontinuierlichen Verbesserung der Sicherheitsregelungen aktiv mitzuwirken.
- Jeder Nutzer ist verpflichtet, ihm bekannte Risiken, Schwachstellen und Sicherheitsvorfälle zu berichten.
- Bei Abwesenheit vom Arbeitsplatz sind die Vorschriften Clear-Screen und Clean-Desk einzuhalten.
- Unbeaufsichtigte Geräte sind adäquat vor Diebstahl bzw. unberechtigter Nutzung zu schützen.

13

Was kann ich als Mitarbeiter konkret tun? I

Klassifikationsstufen im Detail

<u>S1 – Offen</u>	<u>S2 – Intern</u>	<u>S3 – Vertraulich</u>	<u>S4 – Streng Vertraulich</u>
<p>Alle Informationen, bei denen kein Schaden zu erwarten ist, wenn ihre Vertraulichkeit nicht gewährleistet werden kann.</p>	<p>Alle Informationen, die einem größeren Mitarbeiterkreis zugänglich sein sollen, jedoch nicht für Außenstehende bestimmt sind.</p>	<p>Alle Informationen, die innerhalb des Unternehmens nur einem bestimmten Personenkreis oder Fachbereich zur Verfügung stehen dürfen.</p>	<p>Alle Informationen, die in der Regel nur einem eng begrenzten Personenkreis bekannt sein dürfen.</p>
<p>Bsp:</p> <ul style="list-style-type: none">• Bankleitzahlen• Öffentliche Telefonverzeichnisse• Handelsregister• Broschüren und Pressemitteilungen	<p>Bsp:</p> <ul style="list-style-type: none">• Personalnummern• Benutzerkennungen• Organigramme, Rollen- und Aufgabenbeschreibungen• interne Handbücher	<p>Bsp:</p> <ul style="list-style-type: none">• Großteil der Informationen aus fachlichen Anwendungen• Akten zu Geschäftsvorfällen• Quellcode• Mitarbeiterdaten außerhalb der Personalakte	<p>Bsp:</p> <ul style="list-style-type: none">• Vorstandsbeschlüssen• Akten zu geplanten Beteiligungen• Personalakten, Gehaltsinformationen• Personalinformationen für Mitarbeiter

14

Was kann ich als Mitarbeiter konkret tun? III

Konkrete Handlungshinweise

- Lassen Sie niemals vertrauliche Informationen/Dokumente auf Ihrem Schreibtisch, im Flugzeug, in der Bahn oder im Hotel liegen.
- Verlassen Sie nicht den Drucker oder das Faxgerät, wenn Sie vertrauliche Daten senden bzw. Drucken.
- Überprüfen Sie, wer Zugriff zu den Daten benötigt und schränken diesen entsprechend ein.
- Nutzen Sie Verschlüsselungsmechanismen beim Versenden von **Vertraulichen** und **Streng Vertraulichen** Informationen.
- Nutzen Sie unveränderliche Dateiformate (Acrobat PDF) zur Kommunikation mit Geschäftskontakten. (Geeignet für alle Office Dokumente)

Was kann ich als Mitarbeiter konkret tun? IV

Fallen Sie nicht auf Social Engineering rein!

- Schützen Sie unternehmensinterne Informationen in jeder Situation.
- Geben Sie niemals Ihr Passwort heraus (Helpdesk, Systemadministrator).
- Trauen Sie keinem Fremden, auch wenn dieser Ihr Unternehmen sehr gut zu kennen scheint.
- Versichern Sie sich, dass Ihr Gesprächspartner der ist, der er vorgibt zu sein.
- Beschränken Sie die Kommunikation auf die Inhalte, die der Gegenüber wissen muss.
- Vertrauen Sie Ihrer Intuition. Stoppen Sie ein Ihnen verdächtig erscheinendes Gespräch und informieren Sie den Sicherheitsbeauftragten..

Umgang mit Auskunftersuchen II

Ziele der Richtlinie:

- Rechts- und vertragskonformes Verfahren zur Abwicklung von Auskunftersuchen.
- Einhaltung des gesetzlichen Datenschutzes und anderer Verschwiegenheitspflichten.
- Vermeidung von Schäden durch unberechtigte bzw. vertragswidrige Weitergabe von Daten.
- Abwehr von formal fehlerhaften Auskunftersuchen und exakte Einhaltung ergangener Beschlüsse.
- Sicherstellung und Nachweisbarkeit der Auftragskompetenz der handelnden Vertreter des Kunden und mögliche Kostenübernahme.
- Lückenloser, beweisfähiger, schriftlicher oder elektronischer Nachweis über alle internen Verfahrensschritte.
- Rechtmäßige Ermittlungsverfahren dürfen nicht behindert oder vereitelt werden.

17

Umgang mit Auskunftersuchen III

Konsequenzen der Nichteinhaltung:

- Vertragsbruch und / oder Vorwurf der Strafreitelung
- Datenschutzverletzungen
- Schadensersatzansprüche

Angrenzende Sicherheits-Regelungen:

- Datenschutzrichtlinien
- Einschlägige Gesetze

18

Management von Sicherheitsvorfällen I

Vordefinierte Abläufe und Zuständigkeitsregelungen sind notwendig, um die Fähigkeit zur unmittelbaren Reaktion auf Sicherheitsvorfälle zu gewährleisten.

Management von Sicherheitsvorfällen II

Ziele der Richtlinie:

- Schaffung eines Rahmens und spezifischer Regelungen zur Behandlung von Sicherheitsvorfällen.
- Minimierung des möglichen Schadens, Identifikation des Ursprungs und der Ursache, Einleitung geeigneter Maßnahmen (z.B. rechtliche Schritte, technische Lösungen), Eliminierung von Schwächen und Vermeidung ähnlicher Situationen.
- Lernen aus Sicherheitsvorfällen und kontinuierliche Verbesserung der Sicherheitsmaßnahmen, Findung von effektiven Prozessen, Technologien und Rückkopplungsmechanismen für die Prävention von Sicherheitsvorfällen.
- Angemessene Dokumentation der Sicherheitsvorfälle und der ergriffenen Maßnahmen.

Management von Sicherheitsvorfällen III

Auszug der Maßnahmen zur Erreichung der Ziele:

- Definierter und implementierter Sicherheits-Prozess „Management von Sicherheitsvorfällen“.
- Klare Rollen und Verantwortlichkeiten für die Reaktion auf Sicherheitsvorfälle.
- Früherkennung, Meldung und Eskalation von Sicherheitsvorfällen ist als Prozess im QM-System etabliert.
- Existenz eines aktuellen Krisenmanagement-Prozesses im QM-System.
- Existenz eines aktuellen Disaster Recovery Plans und eines entsprechenden Prozesses.
- Beweissicherungsverfahren sind etabliert.
- Periodische K-Fall-Tests zur Simulation von großen Sicherheitsvorfällen oder von Katastrophen.

Management von Sicherheitsvorfällen IV

Konsequenzen der Nichteinhaltung:

- Reaktionen auf Sicherheitsvorfälle können nicht rechtzeitig erfolgen, was zur Erhöhung von Schäden führt

Angrenzende Sicherheits-Regelungen:

- Sicherheits-Prozess „Management von Sicherheitsvorfällen“
- Sicherheits-Richtlinie „Überwachung von Informationsverarbeitenden Komponenten“
- Sicherheits-Rolle „IT-Sicherheitsbeauftragter“

Verhalten bei Sicherheitsvorfällen

23

Verhalten bei Sicherheitsvorfällen

- Brandschutz
- Verhalten gegenüber unbekanntem Personen
 - Ansprechen
 - Verifizieren der Angaben
 - Bei Verdacht: Festhalten und/oder Alarmierung
 - Empfang bzw. Sicherheitsdienst: Hotline **XXXX**
 - Prägen Sie sich besondere persönliche Merkmale ein
- Bei Sicherheitsvorfällen durch Viren oder Hacker Tel.: **XXXX**

24

Maßnahmen bei Verstößen gegen Sicherheitsregelungen I

Maßnahmen sind zur Durchsetzung der Sicherheits-Regelungen und zur Ahndung notwendig, um in Fällen von Verstößen die Wiederherstellung der individuellen Übereinstimmung mit den Sicherheits-Regelungen durchzusetzen.

Maßnahmen bei Verstößen gegen Sicherheitsregelungen II

Ziele der Richtlinie:

- Vermittlung der Ernsthaftigkeit von Verletzungen der Sicherheits-Regelungen
- Definition eines abgestuften Satzes von Konsequenzen bis einschließlich rechtlicher Schritte
- Bereitstellung von Mitteln, um Abweichungen anzugehen
- Abweichungen oder Fehlverhalten muss dokumentiert und entsprechend verfolgt werden
- Entscheidung über Disziplinarmaßnahmen und Reaktionen auf kriminelle Handlungen

Maßnahmen bei Verstößen gegen Sicherheitsregelungen III

Maßnahmen zur Erreichung der Ziele:

- Definition einer Anzahl von Verstößen / Stufen von Verstößen und ein Spektrum von Disziplinarmaßnahmen
- Maßnahmen zur Beweissicherung sind implementiert
- Sicherheitsaudits werden bei sich häufenden Verstößen bzw. bei unklarer Ursache von Verstößen durchgeführt.

Konsequenzen der Nichteinhaltung:

Sicherheit wird nicht ernst genommen, wenn Verstöße keine Konsequenzen nach sich ziehen!

Weitere Richtlinien: Authentifizierung

Ziele:

- Verhinderung von Zugriff auf und Nutzung von Informationswerten für Nutzer, deren Identität nicht verifiziert ist
- Ermöglichung individueller Verantwortlichkeit für Zugriff und Verwendung von Informationswerten und –diensten
- Authentifizierung ist die Basis für Nicht-Abstreitbarkeit, Aktivitätsnachweise, und Durchsetzung von Autorisierungen

Wichtigste Maßnahmen:

- Authentifizierungsmerkmale sind personalisiert
- Beschränkte Zahl von Authentifizierungsversuchen
- Die Weitergabe von Authentifizierungsmerkmalen ist nicht zulässig
- Nutzern, die das Unternehmen verlassen, muss nach ihrem Ausscheiden die Möglichkeit zur Authentifizierung entzogen werden

Weitere Richtlinien: Umgang mit Authentifizierungsmerkmalen

Ziele:

- Schutz der persönlichen Nutzer-Authentifizierungsmerkmale (Passwörter, Schlüssel, Security-Tokens)
- Schutz des Nutzers

Wichtigste Maßnahmen:

- Authentifizierungsmerkmale müssen geheim gehalten werden, sie dürfen nicht im Klartext niedergelegt werden, sie sind ausschließlich für den Nutzer bestimmt!
- Die Verwendung von Authentifizierungsmerkmalen eines anderen Nutzers ist untersagt
- Erzwungene Qualitätsprüfungen der Passworte (z.B. keine Wiederholungen, nichtzyklisch, keine Wörterbuchwörter)
- Erzwungene zeitliche Beschränkung der Passwortgültigkeit

29

Weitere Richtlinien: Clear Screen & Clean Desk

Ziele:

- Schutz von vertraulichen Informationen (Datei- oder Papierform) in Büros und auf Computern
- Schutz von Informationen die sich auf anderen Datenspeichern befinden (PDA, Notebook, USB-Stick, CD-ROM)

Wichtigste Maßnahmen:

- Verschluss von vertraulichen Dokumenten (Schreibtisch)
- Sperren des Rechners („Strg+Alt+Entf“ bei jedem Entfernen vom Arbeitsplatz)
- Schutz von vertraulichen Informationen auf dem Monitor vor Einsichtnahme durch Kunden (z.B. Schließen der Applikation)
- Schutz von Notebooks, PDAs, USB-Sticks, CD-ROM, etc. vor Diebstahl

30

Weitere Richtlinien: Vertragliche Vereinbarungen

Ziele:

- Durchsetzung von individueller Verantwortung und Haftung
- Durchsetzung von Sicherheitsanforderungen gegenüber Geschäftspartnern
- Schaffung einer rechtlichen Grundlage für Verantwortlichkeit, Haftbarkeit und Entschädigung im Falle von Sicherheitsverletzungen

Wichtigste Maßnahmen:

- Aspekte der Informations- und IT-Sicherheit werden in Verträge einbezogen
- Regulierung des Zugangs zu Informationswerten durch Geschäftspartner
- Alle Mitarbeiter, die autorisiert sind, Aufträge und Verträge zu unterzeichnen, sind für die Einbeziehung der Sicherheitsanforderungen in Verträge verantwortlich

31

Weitere Richtlinien: Umgang mit Fremden auf dem Firmengelände

Ziele:

- Keine unberechtigten Personen erhalten Zutritt zu Firmengebäuden bzgl. sensiblen Bereichen
- Vermeidung von Spionage und Diebstahl

Wichtigste Maßnahmen:

- Zutrittskontrolle (Ausweiskontrolle) an den Gebäudeeingängen durch Automaten bzw. Wachpersonal
- Gesonderter Schutz von sensiblen Bereichen (z.B. Büro abschließen)
- Ansprechen von Personen auf dem Firmengelände, die Ihnen unbekannt sind
- Konsequente Besucherbetreuung „von der Pforte bis zur Pforte“

32

**Weitere Informationen und Beispiele entnehmen Sie bitte dem
beiliegenden**

Leitfaden zur Security

Autor: Arno van Züren 1 CFG GmbH
Peter Teichert