Leitfaden Datensicherheit

Sicherheit im Netz

Vertraulichkeit, Integrität und Verfügbarkeit sind die drei wesentlichen Sachziele der Informationssicherheit in Betrieben und Daheim.

Das Internet ist für viele private und berufliche Anwender **das „Tor zur Welt“**, da es einen Informationsaustausch zwischen verschiedenen Nutzern ermöglicht. Viele Geschäftsabläufe werden heute über das Internet abgewickelt. Bankgeschäfte, Versicherungen, der Einkauf von Waren, Urlaubsbuchungen usw. sind üblich geworden. Vielen PC-Nutzern ist nicht klar, dass eine Verbindung zweier oder mehrerer Rechner prinzipiell von beiden Richtungen aus nutzbar ist. Dies gilt erst recht für eine Internetverbindung**. Alle können wie auf einer Postkarte mitlesen.** Was innerhalb von Firmennetzwerken für den firmeninternen Datenaustausch (**L**okal-**A**rea-**N**etwork) sinnvoll, notwendig und erwünscht ist, kann im Internetverkehr zu einer Bedrohung werden.

Aktualisierung der Programme

Die meisten Rechner sind nach dem Neukauf **nicht** auf dem aktuellen Sicherheitsstand. Die Lücken müssen geschlossen werden, weil sonst ein Zugriff eines anderen, eines fremden Rechnerbenutzers, welcher zur gleichen Zeit im Internet ist, ermöglicht wird. Durch eine „Firewall“ (einer „Brandschutzwand“) und eines Antivirenprogramms ist ein gezieltes Abwehren unerwünschter und damit unerlaubter **Zugriffe von außen** zumindest stark eingeschränkt.

Sicherheitslösungen alleine durch die Geräteausstattung *(Hardware)* oder nur durch Programme *(Software)* gibt es nicht. Kenntnisse über technische Lösungsmöglichkeiten um Risiken abwehren zu können, schützen am besten. Regelmäßige Nachfolgeversionen *(Updates)* auf seinen Computer aufzuspielen ist Pflicht! Die Sicherheitspatches *(Patch = Flicken)* der Softwarehersteller müssen deshalb regelmäßig von dessen Internetseite manuell oder automatisch heruntergeladen und aufgespielt werden.

In Firmen ist dazu der Systemverwalter zuständig, Zuhause jeder selbst.

Ohne geeignete technische und organisatorische Lösungen sind über Schwachstellen des Betriebssystems alle Türen für Trojaner, Spyware, Viren, Dialer und Hacker geöffnet.

Der Anwender ist ohne Sicherheitsmaßnahmen völlig durchsichtig für „Alle und jeden“. Zum Schutz der Privatsphäre und der Daten auf dem eigenen Rechner, muss aber ein unberechtigtes Zugreifen auf den eigenen Computer unterbunden werden können.

Risiko Mensch

Auch der Anwender stellt durch unbeabsichtigte Fehlbedienung von Geräten und Programmen ein Sicherheitsrisiko dar. Deshalb ist das programmgestützte Einschränken von Berechtigungen für bestimmte Personenkreise, für bestimmte Mitarbeitergruppen, sinnvoll um die Sicherheit zu verbessern.

Für manche Betriebsstrukturen sind firmeneigene Richtlinien sinnvoll, wenn es um die rechtliche Überprüfbarkeit von Betriebsanweisungen bei Streitigkeiten geht. Der Hessische Kultusminister verlangt deshalb die Erstellung, Fortführung und Umsetzung eines IT-Sicherheitskonzeptes [1]

So heißt es im Amtsblatt 1/10[2]:
„Es müssen geeignete Maßnahmen getroffen werden, um den unberechtigten Zutritt zu schutzbedürftigen Räumen (und Rechnern) *zu verhindern“.*

Betrugsmethoden

im Internet, durch die organisierte Kriminalität, gefährden besonders Nutzer von Online-Diensten. Wer solche Internetdienste nutzt, sollte in besonderem Maße Vorsicht walten lassen, da die organisierte Internetkriminalität in letzter Zeit **sprunghaft zugenommen** hat.

E-Post / E-Mail

Sicherheit beim E-Post Verkehr

Die E-Mail hat sich zu einem seriösen, geschäftsmäßigen Kommunikationsmittel entwickelt. Keine Firma oder Behörde kommt ohne die E-Post heute aus. Da aber diese Post über das weltweite Datennetz verschickt wird, kann jeder mitlesen was gesendet wird. Eine unverschlüsselte E-Post mit vertraulichen Inhalten ist so unsicher wie die alte Postkarte aus dem Urlaub. Jeder kann mitlesen, ob er darf oder nicht! Alle E-Mails werden mehrfach automatisch von Geheimdiensten, Spionageorganisationen oder anderen am Inhalt interessierte Personen mitgelesen.

[1] $10 Abs. 2 Satz 2 HDSG
[2] Bitte lesen Sie das zitierte Amtsblatt!

Öffnen Sie keine **unbekannte** E-Mail-Anhänge. Besonders Dateien mit den Dateiendungen *.exe, können Viren und andere Schadprogramme enthalten. Post mit unbekanntem Absender oder unklarem Betreff, sowie ausländische Absender die Sie nicht kennen, sollten nicht geöffnet, sondern sofort gelöscht werden.[3]

Word-Dateien in Umlauf zu bringen, bzw. Word-Anhänge zu öffnen, kann ein erhebliches Sicherheitsrisiko darstellen, da MS-Word noch immer das am meisten von Kriminellen attackiert Textverarbeitungsprogramm ist. Wenn es dennoch notwendig sein sollte, Word Dateien an Mitarbeiter zu versenden, damit diese daran weiterarbeiten können, sollten diese Dateien mit einem Passwort zum Öffnen versehen sein.

Bitte bedenken Sie, dass alle Grafiken, welche in einem offenen Word-Dokument *(Briefkopf usw.)* vorhanden sind, geradezu wie ein Faksimile zu gebrauchen sind.

Personenbezogene Daten

und Informationen auf einem Computer, welche die Öffentlichkeit nichts angehen, **sollten** bei Internetbenutzung **durch ein** eigenes **Sicherheitskonzept geschützt werden.** Hält man sich nicht daran, muss man damit rechnen, dass jeder fremde, unfreundlich gesinnte Computernutzer diese Daten lesen kann. Die Einrichtung eines **Benutzerkontos,** zum Navigieren im Netz, ist dabei eine Möglichkeit.

Auch **die Benutzung fremder Rechner** zum Tätigen von Geschäften **kann eine Gefahrenquelle darstellen und ist in Schulen in Behörden und am Arbeitsplatz verboten!**

Abhilfe

Wandeln Sie alle **„Info-Dokumente“,** die in einen wie auch immer gearteten Verteiler gestellt werden, in ein **verschlüsseltes PDF-Dokument** um, welches nur die Option zum Ausdrucken hat. Das geht auch schon mit PDF-Umwandlern aus dem Free-Ware Bereich ganz gut *(PDF-Creator etc.).*

Netztipp: http://www.bsi-fuer-buerger.de
https://www.bsi.bund.de

Phishing

ist ein Kunstwort, welches aus „Password“ und „Fishing“ gebildet ist. **Auf gut Deutsch: Passwortklau**. Phishingangriffe sind bereits ein erhebliches Problem. Die Betrüger lotsen ihre Opfer auf eine **gefälschte Netzseite,** auf welcher Passwörter und vertrauliche Daten abgefragt werden. Oft erhalten die Nutzer auch einen E-Brief, in dem vor Sicherheitslücken gewarnt wird. Mit einem Link wird dann auf eine angeblich sichere Seite verwiesen. Diese falschen Seiten sehen jedoch täuschend echt aus.

Ein Tastaturspion, ein so genannter **Keylogger**, der verdeckt im Hintergrund die Tastatureingabe überwacht, um Passwörter und andere Daten zu registrieren, wird von den Gaunern immer öfters eingesetzt. Über den eigenen E-Post-Zugang des betrogenen Nutzers werden dann **Spam-Mails** verschickt, Geschäfte abgewickelt, unsittliche Inhalte verbreitet oder **Geld unbemerkt** von dessen eigenem Internetkonto **abgebucht.**

Viele Unternehmen haben zwischenzeitlich auf die Bedrohung reagiert, indem sie **eine** umfangreiche **Sicherheitsüberprüfung eingeführt** haben, mit der man erkennen kann, ob man sich wirklich auf der offiziellen Internetseite befindet.

Die Passwortdiebe, die Phisher, versenden gefälschte E-Briefe die so aussehen, als kämen sie von der eigenen Internetbank. Auf diesem falschen Brief wird der Empfänger auf eine gefälschte Webseite geführt und aufgefordert, Zugangsdaten, PIN, TAN, usw. einzugeben. Somit bekommen die Betrüger die Möglichkeit, eine Überweisung durchzuführen und das Konto zu plündern.

Noch gefährlicher ist eine Variante des Phishing, das **Pharming**. Die Betrüger ersetzen hierbei die **IP-Adresse** *(**I**nternet-**P**rotokoll-Adresse)* einer bestimmten Netzseite durch eine gefälschte, auf die der Nutzer automatisch geleitet wird, ohne dass dieser es merkt.

Geschäftsverkehr

Durch die Benutzung von Kredit-, Kunden- und Rabattkarten, bzw. deren Nummern hinterlässt der Kunde im Netz elektronische Spuren, z. B. auf Onlineformularen, anhand derer das Einkaufsverhalten nachvollziehbar wird. Mit der Weitergabe eigener Daten sollte man deshalb generell vorsichtig sein. Hier hilft nur ein Passwortschutz und eine technisch sicherere Internetverbindung durch einen **Sicherheitsschlüssel** weiter. Eine solche sichere Netzverbindung erkennt man an den Sicherheitsanzeigen im Netzbrowser.

Datenweitergabe

Zunehmend geraten Kinder und Jugendlich in Schwierigkeiten, weil sie nicht mit den notwendigen Schutzmechanismen vertraut sind, oder die Bedrohung aus dem Netz nicht ernst

[3] Erlass v.27.Nov.09, gült. Verz. Nr. 7200

nehmen. Internetseiten wie sind beliebte Tummelplätze im Netz. Die dort von Jugendlichen auf die Seiten gestellten persönlichen Angaben und Fotos können trotz Passwortvergabe der Nutzer, von Kriminellen und Pädophilen missbraucht werden. Da ist die illegale Adressbeschaffung noch das geringste Problem.

Eltern sollten wissen, welche Seiten ihre Kinder aufrufen und notfalls die Seiten sperren.

Auch sollte man daran denken, dass die Nutzerprofile der genannten und ähnlicher Seiten, bei Bewerbungen vom zukünftigen Boss in Augenschein genommen werden könnten. Fotos von Saufgelagen und freizügiger Kleidung haben schon manchmal zu einer verpassten Anstellung geführt.

Internetquellen beurteilen

Um wenigstens etwas die Quellen, die Seiten des Internetz im Hinblick auf Sicherheit und Seriosität beurteilen zu können, sollte man folgende Fragen mit **„Ja“** beantworten können:

- Gibt es Angaben zum Betreiber der Internetseite? *(Informationen dazu gibt es im Impressum, das jeder Seitenbetreiber haben muss).*
- Werden Quellen/Referenzen angegeben?
- Werden inhaltlich sachliche, ernsthafte und nachprüfbare Informationen geboten?
- Sind die Inhalte zu einem Thema vom Umfang her ausreichend?
- Gibt es neben den allgemeinen Informationen auf der Seite auch Hilfsmittel wie Lexika oder Listen?
- Gibt es auf der Seite eine inhaltlich ausgewogene Sammlung von Verknüpfungen/Links?
- Ist der Schreibstil auf der Seite anspruchsvoll, ohne viele Rechtschreibfehler, die Inhalte und der Satzbau logisch?
- Ist die Seite gut strukturiert und nutzerfreundlich gestaltet?
- Fremdwerbung, kostenpflichtige Zusatzinhalten oder unsinnige Pop-Ups fehlen?
- Die Seite wird regelmäßig aktualisiert oder überarbeitet?
- Gibt es rechtliche Hinweise auf der Seite?
- Die Angaben der Seitenbenutzer werden vom Seitenbetreiber nicht weitergegeben.
- Die allgemeinen Geschäftsbedingungen (AGB) sind leicht zu finden

Netztipps zum Thema:
http://www.internet-abc.de/kinder/
http://www.bsi-fuer-buerger.de/daten

Quellen: siehe Netztipps

Das Datenschutzgesetz

gilt nur für „natürliche“ lebende Menschen *(weitere Infos finden sich im Bundesdatenschutzgesetz und Landesdatenschutzgesetz).*

Die Berechtigung von Organisationen und staatlichen Stellen auf Personendaten zuzugreifen, sind durch **deutsches und europäisches Recht** geregelt. **Behörden** und Organisationen **haben** nämlich auch **ein Recht auf Informationen,** welche für deren Arbeit wichtig sind. So können Polizei und Geheimdienst mit richterliche Erlaubnis Daten von Kriminellen speichern, deren Rechner und Daten beschlagnahmen oder Telefonate von Bürgern mithören *(Terrorbekämpfung, Geldwäsche, Kinder- und Jugendschutz, Drogen, Menschenhandel u.v.m.).*

Das Grundrecht auf informationelle Selbstbestimmung, also das Recht zu entscheiden, welche personenbezogene Daten man weitergeben will, **ist ein Persönlichkeitsrecht.** Es ist eingeschränkt, wenn Allgemeininteressen überwiegen (s. o.).

Um Sozialmissbrauch und Steuerhinterziehung zu verhindern, können Arbeits- und Finanzamt, Sozial- und Einwohnermeldeamt Daten untereinander und mit Banken abgleichen (Umzug, Kfz-Steuer usw.). **Eine unbegrenzte** Aufnahme, Speicherung oder **Verwendung dieser Daten ist** jedoch ausdrücklich **nicht erlaubt.** Wenn der Grund für die Speicherung entfallen ist, müssen alle personenbezogenen Daten gelöscht werden! Firmen, Organisationen und Behörden müssen den unbescholtenen Bürger darüber informieren, welche Daten zu welchem Zweck gespeichert und an welche Stellen die Informationen weitergegeben werden. Auch hat der Bürger das Recht zu erfahren, ob die gespeicherten Daten richtig sind, d. h. er hat ein Auskunftsrecht. Falsche Angaben müssen berichtigt werden. Es besteht ein Anspruch auf Schadenersatz.

Passwortqualität

Die Erstellung eines guten Passwortes ist nicht einfach. Einerseits soll ein Passwort gut merkbar, **andererseits darf es nicht zu offensichtlich** sein. Komplizierte Passwörter, welche man sich aufschreiben muss, sind ungeeignet. **Passwörter die in eine persönliche Verbindung mit dem Anwender gebracht werden können sind genauso schlecht.** Sie sind viel zu leicht zu erraten oder durch Ausprobieren zu knacken. **Vielmehr ist die Länge der Passwortes ein entscheidendes Sicherheitsmerkmal.** Je „wertvoller“ der Inhalt einer Datei ist, umso mehr Zeichen *(Buchstaben, Zahlen, Sonderzeichen)* sollte das Passwort haben. **Gedankenbrücken erleichtern das Behalten des Passwortes.**