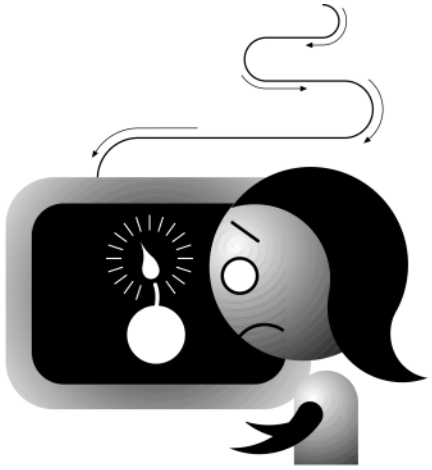
Risiko Internet?

Sicherheitsaspekte bei der Internet-Benutzung

Michael Näf naef@acm.org
www.internet-kompetenz.ch

Februar 2000 – Durch ein verstecktes «Master-Programm» werden Hunderte und Tausende von «Zombie-Rechnern» im Internet gleichzeitig aktiviert, die eine ungeheure Flut von Anfragen an Yahoo! generieren. Innert kürzester Zeit wird Yahoo! – eine der grössten und bestbesuchten Web-Sites der vernetzten Welt – lahmgelegt. Dasselbe Schicksal ereilt auch einige andere der «Big Players» im Internet: Buy.com, ZDNet, eBay, CNN.com und Amazon.

Die Angriffe wurden unter dem Namen «Distributed Denial of Service Attacks» bekannt und sind nicht sonderlich schwer durchzuführen: Man suche eine Zahl ungeschützter Rechner im Internet (davon gibt es genügend) und installiere auf jedem ein frei verfügbares Hacker-Tool wie zum Beispiel Trinoo. Hat man genügend Rechner in der Hand, startet man den Angriff sozusagen auf Knopfdruck.



Mai 2000 – In der Inbox von Tausenden und Abertausenden von unbescholtenen Internet-Benutzern taucht eine E-Mail mit dem Titel «ILOVEYOU» auf, lässt Herzen höherschlagen und bringt Augen zum Leuchten. Doch die vermeintliche Liebeserklärung entpuppt sich als Wurm, ein Programm, das sich selbstständig in einem Computernetzwerk verbreitet und vervielfältigt.

Der ILOVEYOU-Wurm trägt ein Attachment mit einem kleinen Programm mit sich. Beim Öffnen des Attachments kommt das Programm zur Ausführung, kopiert den Wurm an verschiedene Stellen auf der Festplatte und schickt die Mail inklusive Attachment an die Personen aus dem Microsoft-Outlook-Adressbuch weiter. So machte der ILOVEYOU-Wurm unzähligen Benutzerinnen das Leben schwer und brachte die Mail-Infrastruktur mehrerer Firmen zum Erliegen.

August 2000 – Beim Online-Pressedienst «Internet Wire» trifft eine gefälschte E-Mail ein. Die E-Mail stammt angeblich von einer Firma namens Emulex Corp. und informiert über den Rücktritt des CEOs. Ohne den Inhalt zu prüfen veröffentlicht Internet Wire den Bericht. Die Falschinformation wird von anderen Stellen weiterverbreitet. Resultat: Die Aktie von Emulex Corp. fällt von 113 Dollar auf 43 Dollar.

Sicherheit im Internet

Das Internet: schier unerschöpfliche, globale Informationsquelle, blitzschnelles Kommunikationsmedium, hervorragende Plattform für Bildung, Unterhaltung und Gewerbe. Die positiven Seiten des Internets erfreuen sich einer ungebrochenen Medienpräsenz. Ebenso hohe Wellen werfen die problematischen Aspekte im Netz der Netze: Das Internet als Cyber-Sodom voller Pornografie und Viren. An jeder virtuellen Ecke steht ein zerstörungswütiger Hacker, und wer seine Kreditkarteninformationen im Internet preisgibt, wird prompt betrogen.

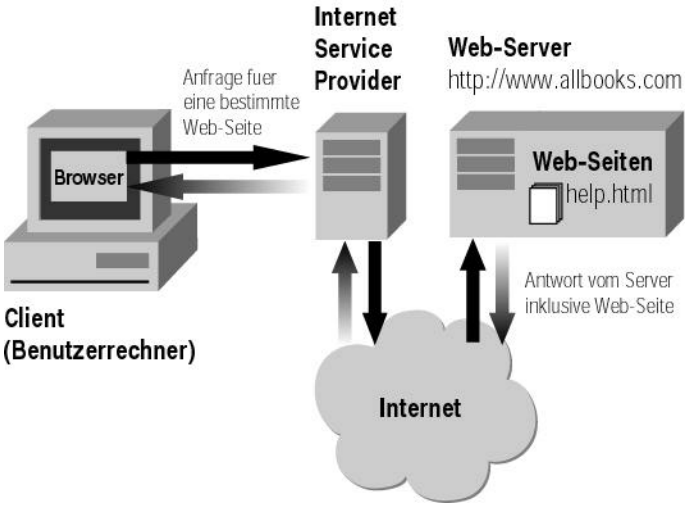
Das Buch «Risiko Internet? Sicherheitsaspekte bei der Internet-Benutzung» von Michael Näf, Patrick Streule und Werner Hartmann bereitet dieser Art der Schwarz-Weiss-Malerei ein Ende. Es wird gezeigt, dass viele Sicherheitsproblematiken des Internets eine Analogie im alltäglichen Leben finden. Die für Internet-Anwender-

innen und -Anwender entscheidenden Aspekte kommen zur Sprache. Es geht nicht darum, die Gefahren im Internet über Gebühr zu betonen. Stattdessen soll der Leserschaft das notwendige Wissen vermittelt werden, um die Risiken im Internet zu beurteilen und einzuordnen.

Der folgende Text greift ausgewählte Themen aus «Risiko Internet?» auf und bietet so einen Überblick über einige sicherheitsrelevante Aspekte bei der Internet-Benutzung.

Das Internet

Das Internet ist ein Zusammenschluss einer unüberschaubaren Zahl von Computern. Jeder Rechner im Netz verfügt über eine eindeutige Adresse. Mit Hilfe dieser Adresse können die Rechner miteinander Kontakt aufnehmen und kommunizieren. Genau genommen sind viele Rechner sogar mit zwei unterschiedlichen Adressen ausgestattet – einer textuellen (zum Beispiel `www.allbooks.com`) und einer nummerischen (zum Beispiel 193.128.12.77).



Man kann die Rechner im Internet in zwei Kategorien einteilen: Die Server stellen ein bestimmtes Angebot zur Verfügung. Sie sind in der Regel (hoffentlich) rund um die Uhr online und beantworten Anfragen von Benutzerinnen. Beispiele für Server: Web-Server, Suchdienste oder News-Server. Die so genannten Clients dagegen bieten typischerweise nichts an, sondern nutzen die Angebote der Server. Die meisten Benutzerinnen verwenden Clients (oder Benutzerrechner), um auf das Internet zuzugreifen.

Im Internet werden verschiedene Dienste angeboten. Die beiden meistgenutzten Dienste sind E-Mail und das World Wide Web (kurz WWW). Für den Zugriff auf das WWW benötigen Benutzer einen Web-Browser. Der Web-Browser ist ein Werkzeug zum Bezug und zur Ansicht von Daten aus dem Internet und insbesondere dem WWW. Konkret hat ein Browser unter anderem die Aufgabe, Web-Seiten auf dem Bildschirm darzustellen. Doch wie findet der Web-Browser eine bestimmte Seite unter den Millionen von Web-Seiten, die im WWW bereitstehen? Zu diesem Zweck sind Web-Seiten durch eine eindeutige Adresse identifizierbar. Diese Adresse wird URL oder Uniform Resource Locator genannt. Ein Beispiel-URL: `http://www.allbooks.com/help.html`. Wie man sieht, taucht im URL die Adresse des Web-Servers auf, der die Web-Seite ausliefert.

Eigenschaften des Internets

Was unterscheidet das Internet vom «normalen» Alltagsleben? Die folgenden drei Punkte sind eine Auswahl von wichtigen sicherheitsrelevanten Eigenschaften des Internets:

- In der Computerwelt ganz allgemein ist eine Tatsache bedeutsam: Information und Informationsträger sind klar voneinander getrennt. Im Alltagsleben ist das unvorstellbar. Beispiel: Bei einer Karrikatur eines Big-Brother-Protagonisten ist die Zeichnung fest verbunden mit dem Papier, auf dem sie gemalt ist. Die Farbe lässt sich nicht vom Papier entfernen, ohne auch das Bild zu zerstören. Anders in der digitalen Welt: Bei einem digitalen Bild steht die Information unabhängig vom Informationsträger zur Verfügung. Die Information lässt sich beliebig kopieren, und es entsteht ein perfektes Duplikat.

- Computer sind schnell! Computer sind geduldig! Ein Computer führt denselben Arbeitsschritt millionenfach durch, ohne sich auch nur einmal zu beschweren. Arbeitsschritte können mühelos automatisiert werden. Von dieser Automatisierbarkeit kann ein Hacker profitieren, um beispielsweise per Internet in einen Computer einzubrechen. Zu diesem Zweck würde der Hacker etwa ein Programm einsetzen, das Passwörter errät, indem es ganze Wörterbücher durchprobiert.
- Ein Rechner im Internet befindet sich in einer äusserst exponierten Situation. Grundsätzlich kann jeder Computer im Netz auf jeden anderen Computer zugreifen. Alle physischen Barrieren verschwinden!

Gefahren im Internet

Welches sind nun die konkreten Gefahren, mit denen eine Internet-Benutzerin im weltumspannenden Datenozean potenziell konfrontiert werden kann? Die drei einführenden Tatsachenberichte geben erste Hinweise: Unbefugte können sich Zugriff auf fremde Rechner verschaffen, E-Mails können gefälscht werden und Viren oder Internet-Würmer können Schaden anrichten.

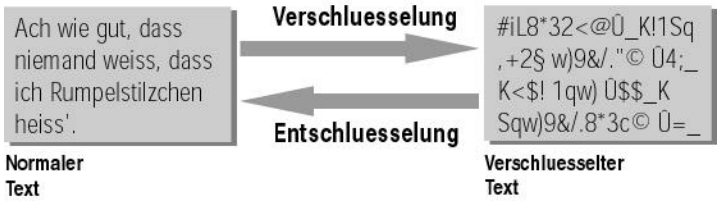
Die restlichen Abschnitte dieses Artikels gehen auf ausgewählte Problemzonen ein, erläutern sie und präsentieren technische Lösungen, die zur Verfügung stehen beziehungsweise Gegenmassnahmen, die Internet-Benutzerinnen treffen können.

Sichere Kommunikation

Mit genügend Aufwand ist im Internet alles «abhörbar». Informationen, die an einen Web-Server geschickt werden, lassen sich grundsätzlich genauso mitverfolgen wie vertrauliche Nachrichten, die via E-Mail versendet werden. Wie also können vertrauliche Informationen trotzdem sicher per Internet übermittelt werden? Die Antwort lautet ...

Verschlüsselung

Durch die Verschlüsselung wird ein Text (oder andere Daten) in einen geheimen Code übersetzt. Der Text wird für Dritte unleserlich und dadurch unbrauchbar gemacht. Neu wird somit beispielsweise nicht mehr die lesbare Botschaft «Ach wie gut, dass niemand weiss, dass ich Rumpelstilzchen heiss'» übermittelt sondern der Buchstabensalat «#iL8*32<@Û_Kè!1Sq,+2§°w)9&/."© Û4;_Kè<$! 1qw) Û$$_Kè Sqw)9&/.8*3ç© Û=_Kè?!^Uza3%». Für Unbefugte ist nicht ersichtlich, was der ursprüngliche Text war.



Der legitime Empfänger hingegen muss in der Lage sein, den Buchstabensalat wieder in die ursprüngliche Form zu bringen. Dazu muss er den Vorgang der Verschlüsselung rückgängig machen. Dieser Umkehrvorgang wird Entschlüsselung genannt.

Für die Ver- und Entschlüsselung von Daten wird eine Zusatzinformation benötigt. Diese Zusatzinformation nennen wir einen Schlüssel.

Verschlüsselung im WWW

Stellen Sie sich vor: Sie bestellen ein Buch bei Amazon und möchten es mit Kreditkarte bezahlen. Doch Sie machen sich Sorgen um die Vertraulichkeit der wertvollen Daten. Was, wenn die Angaben in falsche Hände geraten?

Damit heikle Informationen wie Kreditkartendaten geschützt übermittelt werden, unterstützen die meisten aktuellen Browser und Web-Server eine Technik namens SSL (oder die Variante TLS). SSL bietet unter anderem die Verschlüsselung der zu übertragenden Daten an.

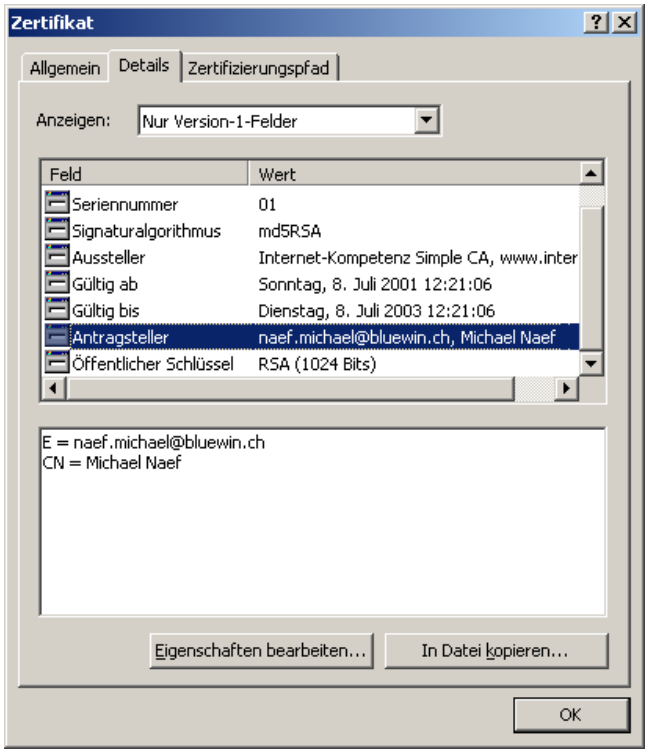
Glücklicherweise bemerken Sie bei der Internet-Benutzung nichts von SSL. Sie brauchen sich um nichts zu kümmern! Und Sie können auf einfache Weise prüfen, ob gerade mit SSL gearbeitet wird und der Datentransport somit verschlüsselt erfolgt. Zwei Merkmale illustrieren den Einsatz von SSL:

- Im Rand des Browser-Fensters wird (beim Netscape Navigator) ein geschlossenes Schnappschloss angezeigt.
- Die aktuelle Adresse im Adressfeld des Browsers beginnt nicht wie üblich mit `http://` sondern mit `https://`.

Aber: Mit der verschlüsselten Übertragung sind nicht alle Probleme gelöst! Mit Hilfe von SSL werden Ihre Kreditkartendaten sicher zum Amazon-Server übermittelt. Doch dort werden die Angaben eingelagert, damit sie beim nächsten Einkauf zur Verfügung stehen. Die Sicherheit der Informationen hängt also auch und entscheidend von einer sicheren Lagerung auf Serverseite ab.

Identifizieren im Internet

Wenn Sie sich im Alltag identifizieren müssen, benützen Sie zum Beispiel einen Pass. Der Pass enthält einige persönliche Angaben sowie ein Foto Ihrer Person. Diese persönlichen Informationen hat eine unabhängige Stelle – das Passbüro – geprüft. Nach der erfolgreichen Überprüfung hat das Passbüro den Pass beispielsweise mit einem Stempel sowie einer Unterschrift bestätigt.



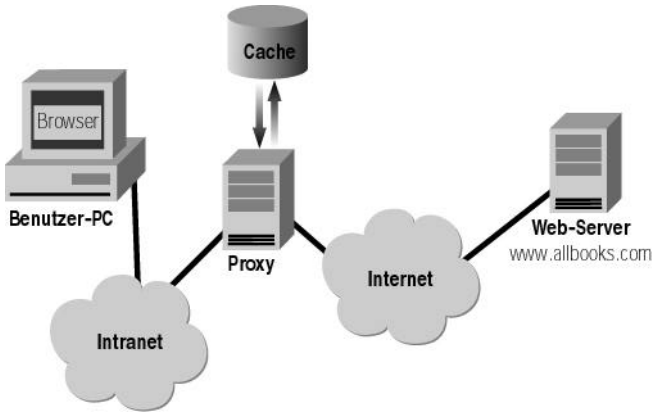
Im Internet müssen wir uns ebenfalls identifizieren können. Zu diesem Zweck gibt es das digitale Äquivalent zu einem Pass: das Zertifikat. Zertifikate dienen als digitale Identitätsausweise. Sie enthalten einige Angaben zu einer Person, zum Beispiel Namen, E-Mail-Adresse, Postadresse oder Geburtsdatum. Die Rolle des Passbüros übernehmen im Internet so genannte Zertifizierungsinstanzen. Sie prüfen die Angaben im Zertifikat und versehen es anschliessend mit einer digitalen Unterschrift, um den Inhalt zu bestätigen.

Entscheidend: Mit einem Zertifikat sind immer auch Verschlüsselungsinformationen gekoppelt. Diese Verschüsselungsinformationen können für zwei wichtige Zwecke eingesetzt werden. Einerseits kann man damit eine Botschaft digital unterschreiben, um die Echtheit des Absenders zu beweisen. Auf diese Weise wird beispielsweise E-Mail-Fälschungen ein Riegel vorgeschoben. Andererseits kann ein Zertifikat an andere Personen verschickt werden. Die Empfänger können die Verschlüsselungsinformationen aus dem Zertifikat anschliessend benutzen, um vertrauliche Nachrichten zu verschlüsseln.

Falls Sie bereits im Besitz eines persönlichen Zertifikats sind, können Sie sich im Browser detaillierte Informationen dazu anzeigen lassen.

Spuren im Netz

Im Internet sind Sie nicht anonym! In der Regel kann jede Ihrer Aktivitäten im Internet mit genügend Aufwand zu Ihnen zurückverfolgt werden, denn Sie hinterlassen an jeder «virtuellen Ecke» Ihre Spuren.



Beispiel Proxy: Viele Computer – ob am Arbeitsplatz oder privat – kommunizieren nicht direkt mit dem Internet. Stattdessen werden alle Internet-Verbindungen über eine Zwischenstation geleitet. Diese Zwischenstation heisst Proxy.

Ein Proxy hat einen gewichtigen Vorteil: Er merkt sich die Seiten, die er einmal heruntergeladen hat und speichert die Seiten bei sich. Beim erneuten Zugriff auf eine bereits gespeicherte Seite muss die Seite nicht aus dem Internet geladen sondern kann direkt vom Proxy ausgeliefert werden. Dadurch wird Zeit gespart.

Ein Proxy ist allerdings nicht immer unproblematisch. Üblicherweise pro-tokolliert ein Proxy sämtliche Benutzeranfragen. Mit Hilfe dieser Angaben lässt sich das Verhalten der Benutzer detailliert verfolgen. In einer Firma beispielsweise kann mit Hilfe des Proxys der gesamte Datenverkehr zwischen Internet und dem firmeninternen Netzwerk mitgeschnitten werden. Anhand der Aufzeichnungen kann geprüft werden, ob die Mitarbeiter das Internet vor allem für die Arbeit oder in erster Linie für private Zwecke einsetzen.

Computerviren

Viren im Alltag sind Krankheitserreger, die sich durch die Veränderung des genetischen Codes von lebenden Zellbestandteilen vermehren. Computerviren vermehren sich ebenfalls selbstständig, indem sie andere Programme befallen und verändern. Viele Computerviren führen nichts Gutes im Schilde und beschädigen ein infiziertes Computersystem. Andere Viren sind weniger bösartig und begnügen sich mit unschädlichen, aber nervenaufreibenden Störaktionen. An dieser Stelle soll eine spezielle Art von Viren vorgestellt werden: Makro-Viren.

Word-Makro-Viren

Ein Dokument aus einer typischen Textverarbeitung wie Microsofts Word würde man eigentlich als unproblematisch einstufen. Schliesslich kommt in einem Word-Dokument nichts anderes vor als Text- und Formatierungszeichen sowie vielleicht eine Tabelle und das eine oder andere Bild. Doch der Schein trügt! Word beinhaltet eine so genannte Makro-Programmiersprache.

Ursprünglich dienten Makros dazu, immer wiederkehrende Aktivitäten zu automatisieren. Unterdessen ist Microsofts Makrosprache aber derart fortgeschritten, dass die Möglichkeiten fast unbegrenzt sind. Word-Dokumente sind daher nicht immer ungefährlich. Wer ein Word-Dokument öffnet, läuft Gefahr, gleichzeitig ein Makro-Virus zu aktivieren.

Schutz vor Makro-Viren

Wie können Sie sich vor Makro-Viren schützen? Drei Vorschläge:

- Sie besorgen sich ein Antivirenprogramm und lassen jedes neue beziehungsweise unbekannte Dokument überprüfen.
- Sie öffnen keine Word-Dokumente mehr, die Sie von Dritten erhalten haben. Wenn Sie ein Word-Dokument per E-Mail erhalten, so verlangen Sie eine reine Textfassung des Dokuments.
- Bei neueren Word-Versionen können Sie einen Makrovirus-Schutz aktivieren. Fortan werden neu geöffnete Dokumente zunächst auf Makros geprüft. Falls Makros vorkommen, haben Sie die Wahl, ob sie ausgeführt werden sollen oder nicht.

Hoaxes – Pseudoviren

> Subject: Good Times!
>
> Here is some important information. Beware of a file called "Good Times". Be careful out there. There is a virus on the Internet being sent by e-mail. If you get anything called "Good Times", DON'T read it or download it. It is a virus that will erase your hard drive. Forward this warning to all your friends. It may help them a lot.

Haben Sie auch schon eine Nachricht wie die nebenstehende in Ihrer Inbox vorgefunden?

Es handelt sich hier um einen Hoax (oder Pseudovirus). Hoaxes sind Falschmeldungen. Die «Good Times»-Warnung ist ein typisches Beispiel für einen Hoax. Es gibt kein echtes Virus namens «Good Times».

Viele Hoaxes funktionieren wie Kettenbriefe. Sie legen den Lesern nahe, die Warnung an ihre Bekannten zu verschicken, um auch sie vor Schaden zu bewahren. Insofern kann die Falschmeldung selbst als ein Virus angesehen werden. Pseudoviren richten Schaden an, indem sie die Zeit der Leser sowie technische Ressourcen für die Bearbeitung und Übermittlung verschwenden.

Was tun? Ignorieren! Es kommt höchst selten vor, dass Meldungen dieser Art der Wahrheit entsprechen. Im Zweifelsfall kann man auf im WWW publizierten Hoax-Listen nachschauen, ob es sich um einen Hoax handelt.

Was ist mit …?

Der sehr kurze Überblick zum Thema «Sicherheit im Internet» ist damit abgeschlossen. Sie haben einen Eindruck erhalten von den Problemen, die sich stellen und den Lösungen, die sich anbieten. Viele Fragen sind jedoch offen geblieben. Zum Beispiel:

- Wie kann man sich den Vorgang der Ver- und Entschlüsselung von Daten an konkreten Beispielen veranschaulichen? Was geschieht bei der Verschlüsselung mittels SSL im WWW hinter den Kulissen?
- Wie sieht eine digitale Unterschrift aus? Wie funktionieren digitale Zertifikate genau und welche Zwecke erfüllen sie? Wo im WWW trifft man auf Zertifikate im Zusammenhang mit Diensten wie WWW oder E-Mail?
- Welche Möglichkeiten zur Zugriffskontrolle auf ein Computersystem oder andere elektronische Ressourcen gibt es?
- Wie kann man im Internet bezahlen? Welche aktuellen Ansätze für elektronische Zahlungssysteme gibt es, wie arbeiten diese, und welches sind die Schwachstellen?
- Welche Spuren hinterlassen Sie bei der Internet-Benutzung, und was können Sie dagegen tun?
- Welchen Risiken sind Sie im Zusammenhang mit Programmen (Shareware, Freeware, Java-Applets, JavaScript, Visual Basic Script usw.) aus dem Netz ausgesetzt? Welche Massnahmen bieten sich gegen Computerviren an?
- Was ist «Spamming», und wie soll darauf reagiert werden? Wie lassen sich problematische Inhalte aus dem Internet ausfiltern?

Michael Näf
Patrick Streule
Werner Hartmann

Risiko Internet?
Sicherheitsaspekte bei der Internet-Benutzung

Orell Füssli Verlag, Zürich, 2000
ISBN 3-280-02770-5

Alle aufgelisteten und eine ganze Fülle weiterer Fragen werden im Buch mit dem Titel «Risiko Internet?» beantwortet.

Das Buch nähert sich dem Thema «Sicherheit im Internet» konsequent aus der Anwenderpespektive und legt besonderes Gewicht auf die Vermittlung von langlebigen Konzepten. Anhand von Analogien aus dem Alltag wird gezeigt, dass es sich bei den vermeintlich neuartigen Problemen oft um altbekannte handelt, die im Internet eine neue Spielform gefunden haben.

Die Leserinnen und Leser können das Wissen erwerben, das für eine selbstständige Beurteilung der Risiken im Internet notwendig ist. Ziel ist es, mit den tatsächlichen Risiken des Internets nüchtern und kompetent umgehen zu können.

Das Buch richtet sich an einen breiten Personenkreis von Internet-Anwendern und –Anwenderinnen, die über grundlegende Fertigkeiten und Erfahrungen mit dem Internet verfügen und sich im Hinblick auf eine sichere Nutzung der Internet-Dienste weiterbilden wollen. «Risiko Internet?» richtet sich somit an alle, die im Berufsleben oder privat das Internet verantwortungsbewusst als Werkzeug einsetzen möchten. Die Erläuterungen sind bewusst einfach gehalten, auf unnötige technische oder mathematische Details wird verzichtet.