Checkliste: Schutz für Unternehmen

„Wird die Bedrohung für unser Netzwerk nicht übertrieben? Und wann lohnen sich unsere Investitionen in die Computersicherheit?“ – Diese Punkte werden oft zur Diskussion gestellt, wenn IT-Verantwortliche in Unternehmen nach dem Sinn oder Unsinn von Sicherheitsmaßnahmen für Computer und Netzwerke gefragt werden. Die Bedrohung aus dem Internet erscheint zu theoretisch und wird daher nicht ernst genommen. Erst wenn Sicherheitsvorfälle eingetreten sind, werden im Nachhinein (und damit zu spät) Mittel für geeignete Schutzmaßnahmen bewilligt.

Die Entwicklung der letzten Jahre zeigt jedoch sehr deutlich, dass gerade Investitionen in diesen sensiblen Bereich notwendig und sinnvoll sind.

Am besten, Sie gehen einfach diese Checkliste Punkt für Punkt durch und nehmen die nötigen Anpassungen an Ihrem IT-System vor! Durch das Schließen dieser wichtigsten Sicherheitslücken können Sie schon bald von einem maximalen Schutz profitieren.

- Unternehmen jeglicher Größenordnung sind in immer größerem Umfang von der EDV abhängig. Ausfallzeiten, die beispielsweise durch Computerviren verursacht werden, erzeugen massive Kosten. Hinzu kommen indirekte Kosten, wie z. B. durch den Imageverlust gegenüber Geschäftspartnern und Kunden.

  Gecheckt: ☐

- Die Absicherung eines Unternehmensnetzwerks ist eine Aufgabe, die Zeit, personelle Ressourcen und damit auch Geld erfordert. Dies steht im Gegensatz zu der Reduzierung von IT-Personal und IT-Budgets in vielen Unternehmen.

  Gecheckt: ☐

- Die Anzahl der sicherheitsrelevanten Vorfälle hat in den letzten Jahren massiv zugenommen. So berichtet das CERT (http://www.cert.org/stats/cert_stats.html) – eine der wichtigsten weltweiten Institutionen zur Beobachtung der Internet-Kriminalität – im Jahr 1993 von insgesamt 1.334 so genannter Incidents, im Jahr 1998 bereits von 3.734 und schließlich im Jahr 2003 von 137.529.

  Gecheckt: ☐

- Mittlerweile verfügt fast jedes Unternehmen über eine permanente Internet-Anbindung, und viele Mitarbeiter setzen mobile Geräte oder Heimarbeitsplätze ein, was das Risiko zusätzlich vergrößert.

  Gecheckt: ☐

- Angriffe aus dem Internet erfolgen oft automatisiert. Viren und Würmer suchen sich keine speziellen Opfer aus! Den typischen Hacker, der ausschließlich in Großunternehmen eindringt und sich dort bereichert, gibt es im Kino häufiger als in der Realität. Dies ist außerdem nur ein spezieller Bereich der Computerkriminalität. Jedes Unternehmen kann das Opfer eines Angriffs aus dem Internet werden!

  Gecheckt: ☐

- Sobald eine Verbindung zwischen dem Unternehmensnetzwerk und dem Internet besteht, ist es Bestandteil einer weltweiten Web-Gemeinschaft. Ein ungeschütztes Netzwerk kann von Hackern oder Spammern dazu missbraucht werden, andere Systeme anzugreifen oder zu belasten. Ein wirksamer Schutz vor kriminellen Machenschaften im weltweiten Computernetz kann nur dann funktionieren, wenn sich alle Beteiligten engagieren und in geeignete Gegenmaßnahmen investieren!

Gecheckt: ☐

Fazit: Auf Investitionen in die Computer- und Netzwerk-Sicherheit kann in der heutigen Zeit kein Unternehmen verzichten!

Die Mitarbeiter – der Schlüssel zum Erfolg

Ein wichtiger Faktor wird in vielen Unternehmen immer noch außer Acht gelassen: die Information und Schulung der Mitarbeiter!

Technische Sicherheitsmaßnahmen alleine reichen nicht, wenn sich die Mitarbeiter nicht an Regeln und Verhaltensempfehlungen halten. Der allzu sorglose Umgang mit Passwörtern ist nur ein Beispiel für Probleme, die sich mit Technik allein nicht in den Griff bekommen lassen. So sind alle Sicherheitstipps nutzlos, wenn sie nicht allen Kollegen bekannt sind und angewendet werden.

Zu einem erfolgreichen Sicherheitskonzept gehören daher auch Schulungen und Informationen für die Mitarbeiter. Diese Maßnahmen müssen regelmäßig wiederholt und aktualisiert werden, um einen gleichmäßig hohen Sicherheitslevel im Unternehmen zu gewährleisten.

Information

Leider lassen sich die Hacker & Co. der Computerwelt immer wieder neue Tricks einfallen, um Systeme anzugreifen und zu manipulieren. Ein Schutz vor Computerkriminellen, der heute noch ausreichend ist, kann in einigen Wochen leicht zu umgehen sein – es herrscht ein steter Wettlauf zwischen Verteidigern und Angreifern.

Die gute Nachricht: Mit einigen grundlegenden Gegenmaßnahmen und vertretbarem Aufwand kann man die Sicherheit seines PCs deutlich verbessern und das Risiko eines erfolgreichen Angriffs verringern!

Dazu ist es allerdings erforderlich, sich immer wieder mit diesem Thema zu beschäftigen. Nur wer sich ständig über den neuesten Stand der Schutztechnologien und der Angriffsszenarien informiert, kann sich effektiv verteidigen. Lassen Sie sich von externen Sicherheitsspezialisten beraten, welche Maßnahmen für Ihren Computer zu empfehlen sind. Kollegen und Sicherheitsbeauftragte aus anderen Unternehmen können ebenfalls wertvolle Tipps beisteuern.

Darüber hinaus werden mittlerweile im Internet aktuelle und leicht verständliche Informationen und Anleitungen bereitgestellt. Besuchen Sie daher regelmäßig diese oder andere Sicherheits-Webseiten, damit Sie immer auf dem neuesten Stand bleiben.

Checkliste: Schutz für Unternehmen

Sicherheit 1-2-3

Auch wenn Sie vielleicht (noch) kein Experte für Computersicherheit sind – mit drei einfachen Maßnahmen können Sie die Computer in Ihrem Netzwerk deutlich sicherer machen:

1. Setzen Sie immer eine möglichst aktuelle Version des Betriebssystems und der Anwendungsprogramme ein. Alle Hersteller veröffentlichen regelmäßig Aktualisierungen (Patches), die vorhandene Fehler korrigieren und potenzielle Sicherheitslücken schließen. Diese Patches sollten schnellstmöglich nach der Veröffentlichung installiert werden.
2. Verwenden Sie auf allen Rechnern im Netzwerk ein Antiviren-Programm, und aktualisieren Sie es regelmäßig. Tests und Empfehlungen von guten Schutzprogrammen werden regelmäßig in Computerzeitschriften oder im Internet veröffentlicht.
3. Schützen Sie Ihr Netzwerk durch eine leistungsfähige aktuelle Firewall. Die einzelnen Rechner sollten zusätzlich durch eine lokal installierte Firewall (Personal Firewall) abgesichert werden – insbesondere, wenn es sich um mobile Geräte wie Notebooks handelt. Eine Firewall funktioniert wie ein digitaler Schutzwall um das Netzwerk oder den PC und kontrolliert die Kommunikation mit dem Internet.

Wenn Sie diese drei Maßnahmen beachten, haben Sie schon viel erreicht! Detailliertere Informationen und Handlungsempfehlungen haben wir nachfolgend für Sie zusammengestellt.

Gecheckt: ☐

Neu schützt ...

Noch einmal: IT-Sicherheit ist ein ständiger Wettlauf zwischen Angreifer und Verteidiger! Ein wichtiger Schritt, um Ihre persönliche Sicherheit zu verbessern, besteht darin, alle eingesetzten Produkte regelmäßig auf den neuesten Stand zu bringen. Auch wenn sich die IT-Industrie seit Jahren sehr bemüht, die Anzahl der Schwachstellen in Software und Hardware zu reduzieren, kann man trotzdem nicht immer von einem absolut fehlerfreien Produkt ausgehen. Moderne Betriebssysteme und Anwendungen bestehen aus mehreren Millionen Zeilen Programmcodes – daher sind potenzielle Schwachstellen nicht auszuschließen. Viele Fehler treten auch nur in bestimmten Konstellationen oder im Zusammenspiel mit anderen Komponenten auf, können also nicht sofort aufgespürt werden. Sobald Fehler oder Lücken entdeckt werden, begeben sich die Hersteller an die Korrektur des Problems und stellen eine Aktualisierung – den Patch – zur Verfügung. Dieser Patch sollte nun schnellstmöglich von Ihnen eingesetzt werden, um das Problem zu beseitigen und die Sicherheitslücke zu schließen. Nachfolgend haben wir einige wichtige Tipps rund um das Thema Patchen zusammengestellt:

- Verschaffen Sie sich einen genauen Überblick über die Hardware und Software, die Sie einsetzen. Für viele Produkte, die Sie verwenden, werden sehr wahrscheinlich regelmäßig Aktualisierungen von den Herstellern veröffentlicht – zum Beispiel für das Betriebssystem, die Anwendungssoftware, das Virenschutzprogramm und die Firewall, die Sie hoffentlich einsetzen, usw. Um den bestmöglichen Schutz zu erreichen, müssen alle diese Komponenten auf dem neuesten Stand sein!

Gecheckt: ☐

- Viele aktuelle Betriebssysteme und auch Anwendungsprogramme verfügen heute über automatische Update-Komponenten. Über eine Internet-Verbindung werden so die veröffentlichten Aktualisierungen auf Ihren Rechner geladen und installiert. So wird das regelmäßige Patchen der Computer automatisiert und kann nicht vergessen werden.

Gecheckt: ☐

- Wenn Sie ein Systemmanagement-Programm zur automatisierten Verteilung von Software einsetzen, können auf diesem Weg schnell und Kosten sparend Aktualisierungen vorgenommen werden.

Gecheckt: ☐

- Besteht diese Möglichkeit nicht, sollten Sie sich auf den Internet-Seiten des Herstellers informieren, ob eine Mail oder ein Newsletter verschickt wird, der auf eine veröffentlichte Aktualisierung hinweist. In diesem Fall sollten Sie Ihre E-Mail-Adresse hier eintragen. Bietet der Hersteller diesen Service nicht an, lohnt es sich, auf das Angebot der bekannten Sicherheits-Webseiten zurückzugreifen. Hier wird in der Regel hersteller- und produktneutral informiert.

Gecheckt: ☐

Ein wichtiger Punkt beim Thema Software-Aktualisierung ist die Fragestellung, ob wirklich jeder Patch installiert werden muss. In diesem Zusammenhang wird häufig auf mögliche Probleme nach der Patch-Installation verwiesen. Diese Fragestellung kann leider nicht allgemeingültig beantwortet werden. Natürlich existieren Abhängigkeiten zwischen Patchen und anderen Programmen. Daher sollten Unternehmen zuerst Tests durchführen und erst dann eine Verteilung im gesamten Netzwerk starten.

Allerdings sollte der Zeitraum zwischen Veröffentlichung und Installation eines Patches nicht allzu groß werden. Der Grund für diese Empfehlung ist die Gefahr, dass ein Hacker durch den verfügbaren Patch erst auf die potenzielle Schwachstelle im Produkt hingewiesen wird. Durch eine Technologie, die sich „Reverse Engineering“ nennt, können findige Angreifer sehr schnell aus dem Patch auf die ursprüngliche Lücke schließen und so einen Angriffscode entwickeln. Dies ist nicht nur ein theoretisches Problem, sondern tritt in der Praxis immer häufiger auf.

Viren, Würmer und Trojaner

Ein weiterer wichtiger Baustein für einen effektiven Schutz gegen Hacker ist ein wirkungsvoller und aktueller Virenschutz!

Während in der Anfangszeit der Computerviren die Infektion eines PCs fast ausnahmslos über Datenträger wie Disketten oder CD-ROMs erfolgte, sind die möglichen Übertragungswege heute sehr viel zahlreicher. Durch das Internet und die nahezu flächendeckende Verbreitung von E-Mail kann eine Virenepidemie sehr schnell unglaublich viele Systeme erreichen. Mit einem ungeschützten Rechner im Internet zu surfen, muss mittlerweile als grob fahrlässig eingestuft werden. Was muss man tun, um den eigenen PC zu schützen?

- Installieren Sie auf jedem System ein Antiviren-Programm. Die Schutzsoftware muss zu dem jeweiligen Rechner „passen“ – also beispielsweise keine Client-Version auf einem Server einsetzen.

Gecheckt: ☐

- Der Virenschutz muss regelmäßig aktualisiert werden. Ein veralteter Virenscanner ist absolut nutzlos! Die Marktführer in diesem Bereich aktualisieren die so genannten Virensignaturen oder auch „Pattern“ mittlerweile mehrmals täglich. Daher sollten die Virenschutz-Programme so konfiguriert werden, dass sie selber nach Updates auf den entsprechenden Servern suchen.

Gecheckt: ☐

Checkliste: Schutz für Unternehmen

- Denken Sie an die neuen Gerätetypen, die Sie einsetzen: Moderne Mobiltelefone, PDAs (Taschencomputer) oder auch Organizer bieten die Möglichkeit, Dateien zu transportieren und auszutauschen. Auch so können Computerviren auf Ihren PC eindringen.

  Gecheckt: ☐

- Löschen Sie verdächtige Mails, ohne sie zu öffnen! Nicht probehalber öffnen – nicht weiterleiten – keine Vorschau – einfach löschen!

  Gecheckt: ☐

- Prüfen Sie, ob es in den von Ihnen eingesetzten Programmen zusätzliche Sicherheitseinstellungen gibt. In vielen Programmen können z. B. wiederkehrende Aufgaben in so genannten „Makros" automatisiert ausgeführt werden. Diese eigentlich hilfreiche Eigenschaft haben in der Vergangenheit viele Virenprogrammierer ausgenutzt, um Makroviren zu entwickeln – daher verfügen die meisten aktuellen Programmversionen über die Möglichkeit, die Makrosicherheit zu konfigurieren. Hier sollte immer die höchstmögliche Stufe eingestellt sein.

  Gecheckt: ☐

- Ein ähnliches Problem gibt es bei der Internet-Nutzung mit einem Browser: Um das Web interessanter zu gestalten und leistungsfähigere Internet-Anwendungen möglich zu machen, werden mit Hilfe spezieller Entwicklungstechnologien wie JavaScript oder ActiveX aktive Inhalte für Internet-Seiten entwickelt. Bestimmte Anwendungen, die Sie auch sicherlich schon genutzt haben, wären ohne diese Technologie nicht möglich. Leider sind auch die aktiven Inhalte mittlerweile zu einem Gefahrenpotenzial geworden. Verschiedene Sicherheitsexperten empfehlen daher zurzeit, die aktiven Inhalte weitestgehend im Browser zu deaktivieren oder dem Anwender zumindest eine Warnmeldung bzw. eine Eingabeaufforderung anzuzeigen. Alternativ unterstützen einige Internet-Browser die Aufteilung des Internets in unterschiedliche Zonen. Für die einzelnen Zonen können verschiedene Sicherheitseinstellungen konfiguriert werden. Damit ist es möglich, für vertrauenswürdige Internet-Seiten (z. B. Ihre Bank) die aktiven Inhalte zuzulassen.

  Gecheckt: ☐

- Dateien, die Sie aus dem Internet erhalten, sollten immer zuerst auf der Festplatte gespeichert und mit dem Virenscanner geprüft werden. Das direkte Öffnen oder Ausführen einer Datei ist sehr gefährlich und sollte unter allen Umständen vermieden werden.

  Gecheckt: ☐

- Sollten auf einer Webseite merkwürdige Dialogboxen angezeigt werden oder sich ungewollt neue Fenster öffnen, betätigen Sie keinesfalls die angezeigten Schaltflächen, sondern schließen Sie die Fenster mit dem Schließ-Symbol der von Ihnen eingesetzten grafischen Benutzeroberfläche. (In den allermeisten Fällen das Symbol in der rechten oberen Ecke des Fensters – bei Microsoft Windows ist es das Kreuz.)

  Gecheckt: ☐

Checkliste: Schutz für Unternehmen

Der Schutzwall um den Rechner und das Netzwerk – die Firewall

Ein extrem wichtiger Baustein im Schutz gegen Hacker und unerlaubte Eindringlinge ist die Firewall. Sie dient dazu, nur bestimmte Kommunikationskanäle zu öffnen und andere zu blockieren. Firewalls sind in den unterschiedlichsten Ausführungen und Bauformen verfügbar – es gibt sie als Kombination von Hard- und Software und als reine Software-Lösung.

Unternehmensnetzwerke sind in der Regel durch mindestens eine Firewall am Übergang vom internen Netzwerk zum Internet geschützt. Bei komplexeren Netzwerkdesigns kommen auch mehrere Firewall-Systeme zum Einsatz. Firewalls wurden in den letzten Jahren erheblich weiterentwickelt und von den Herstellern in ihrer Funktionalität erweitert. Wenn Sie in Ihrem Unternehmen ältere Systeme einsetzen, sollten Sie prüfen, ob sie den heutigen Anforderungen noch genügen. In jedem Fall ist eine regelmäßige Überwachung der Firewall und Auswertung der Protokolldateien erforderlich, um eventuelle Sicherheitsprobleme schnell aufzudecken.

Durch die Weiterentwicklung der Internet-Nutzung und die Entstehung neuer Bedrohungsszenarien ist der zusätzliche Einsatz von „Personal Firewalls“ sehr wichtig geworden. Diese persönlichen Firewalls bestehen in der Regel ausschließlich aus Software und sind entweder Bestandteil aktueller Betriebssysteme oder zusätzliche Applikationen. Die lokale Installation einer Personal Firewall auf Unternehmens-PCs kann das Sicherheitskonzept für Ihr Netzwerk sinnvoll erweitern.

Egal welche Technologie Sie einsetzen – eine Firewall ist für die heutige Internet-Nutzung unverzichtbar geworden:

- Eine Firewall ist nur ein Bestandteil eines Sicherheitskonzepts! Sie ist unverzichtbar – muss aber auch durch andere Sicherheitstechnologien wie Virenschutz und Softwareaktualisierung ergänzt werden.

  Gecheckt: ☐

- Personal Firewalls, die auf den PCs arbeiten, können nach der Installation „lästig“ werden, da sie sich ständig mit Dialogboxen bei den Anwendern meldet. Dies ist allerdings notwendig, da die Firewall nun in einer „Lernphase“ ist und analysiert, welche Internet-Kommunikation notwendig ist. Die angezeigten Fragen sollten von den Usern aufmerksam durchgelesen werden. Prüfen Sie, ob tatsächlich eine Internet-Kommunikation von Ihnen angefordert wurde. Sie werden feststellen, dass die Anzahl der Eingabeaufforderungen nach einigen Tagen drastisch nachlässt.

  Keinesfalls sollte aus diesem Grund eine Personal Firewall deaktiviert oder deinstalliert werden!

  Gecheckt: ☐

Die E-Mail-Flut beherrschen – Schutz vor Spam: E-Mail-Programm

Die meisten aktuellen Versionen der E-Mail-Programme verfügen über so genannte „Spam-Filter“ oder „Junk-Mail-Filter“. Auch wenn jeder Hersteller unterschiedliche Kriterien verwendet, sind diese Filter mittlerweile sehr gut dazu geeignet, einen großen Anteil der unerwünschten Post aus Ihrem Posteingang fernzuhalten.

Wenn Sie den Spam-Filter aktivieren, sind in der Regel unterschiedliche Filteroptionen verfügbar. Weitere Hinweise zur Konfiguration finden Sie in der Regel in der Anleitung oder Online-Hilfe des Herstellers.

Zu Beginn sollten Sie den Filter auf eine niedrigere Stufe einstellen und Spam-Mails nicht sofort löschen, sondern zunächst markieren oder automatisiert in einen separaten Ordner verschieben. Nach den ersten Erfahrungen kann der Filter dann Schritt für Schritt auf strengere Kriterien umgestellt werden. So vermeiden Sie, dass durch den Filter versehentlich wichtige Mails aussortiert werden.

Da sich die Spam-Versender immer wieder neue Ideen einfallen lassen, müssen auch die Spam-Filter aktualisiert werden. Informieren Sie sich regelmäßig beim Hersteller Ihres E-Mail-Programms, ob Aktualisierungen für den Spam-Schutz angeboten werden.

Ein anderer wirkungsvoller Schutz sind Empfänger- bzw. Versenderlisten, die in Ihrem E-Mail-Client gepflegt werden können. Auch dieses Leistungsmerkmal ist in fast allen aktuellen Mail-Programmen zu finden. Über diese Listen können Sie definieren, wer Ihnen Nachrichten zukommen lassen darf („Whitelist") – oder auch wer das auf keinen Fall tun darf („Blacklist"). Leider sind diese Aufstellungen nur wirkungsvoll, wenn sie regelmäßig gepflegt werden. Außerdem ist diese Schutzmaßnahme nur dann wirksam, wenn die Absenderadressen nicht gefälscht sind.

Zusätzliche Spam-Schutzsoftware

Mittlerweile gibt es eine große Anzahl verfügbarer Software-Produkte, die Sie effektiv vor Spam schützen können. Bevor Sie sich aber zum Kauf einer solchen Anti-Spam-Lösung entschließen, sollten Sie zunächst alle Möglichkeiten nutzen, die bereits in Ihrer Software vorhanden sind bzw. die Ihnen der Internet-Provider anbietet.

Wenn diese Schutzmechanismen nicht die gewünschte Wirkung erzielen oder Sie diese für nicht mehr ausreichend halten, können auch Zusatzprodukte in Betracht gezogen werden. In den gängigen Fachzeitschriften werden ständig aktuelle Spam-Schutz-Werkzeuge getestet.

E-Mail-Anbieter

Die meisten Anbieter von kostengünstigen oder kostenfreien E-Mail-Diensten stellen mittlerweile ebenfalls Spam-Filter zur Verfügung. Sie können diese Hilfsmittel guten Gewissens nutzen, um den Empfang von unnützer und lästiger elektronischer Post zu verringern.

Einige Anbieter ermöglichen es sogar, die Absender solcher Mails online zu melden. Die Mitarbeit aller Anwender hilft den Internet-Providern, schwarze Schafe zu identifizieren und die Spam-Filter effizient weiterzuentwickeln. Dadurch helfen sie sich und anderen Internet-Anwendern, das Spam-Problem in den Griff zu bekommen.

Proaktives Verhalten

Auch durch den bewussten Umgang mit dem Medium E-Mail können Sie dazu beitragen, dass die Anzahl der Spam-Mails in Ihrem und in anderen Postfächern nicht ständig weiter wächst.

Ihre E-Mail-Adresse gehört zu Ihren persönlichen Daten! Sie sollte also nur den Menschen zur Verfügung stehen, von denen Sie auch Mails empfangen möchten!

Einige kleine Verhaltensempfehlungen können maßgeblich dabei helfen, dieses Ziel zu erreichen und weitestgehend ohne unerwünschte elektronische Post zu leben:

- Verwenden Sie mehrere E-Mail-Adressen bzw. Postfächer. Eine Adresse für die normale private oder geschäftliche Kommunikation – eine zweite Anschrift für alle anderen Zwecke. Diese Adresse können Sie zum Beispiel bei Online-Bestellungen, Registrierungen, Newslettern,

Gewinnspielen, Anforderungen von Warenproben und ähnlichen Einsatzszenarien verwenden. Ein wichtiger Tipp, denn manche Anbieter von Waren und Dienstleistungen könnten die Datenschutzbestimmungen leider nicht sehr ernst nehmen und Adressen an Spam-Versender weitergeben.

Gecheckt: ☐

- Hinterlassen Sie im Internet (z. B. in Diskussionsforen oder Gästebüchern) niemals Ihre E-Mail-Adresse in korrekter Schreibweise – also „Absendername@E-Mail-Domäne". Es gibt automatisierte Programme, die das Internet nach solchen lesbaren E-Mail-Adressen durchforsten und diese an Spam-Versender zurückmelden. Durch kleine Tricks können Sie solche „Spionageroboter" austricksen: Ersetzen Sie z. B. das @-Zeichen durch die Buchstabenfolge „-at-" – schon funktioniert das automatisierte Adressensammeln nicht mehr. Eine andere Möglichkeit besteht darin, an beliebiger Stelle in der E-Mail-Adresse einen Text wie „-keinSpam-" einzufügen. Jemand, der Ihnen wirklich antworten möchte, wird sofort erkennen, was zu tun ist.

Gecheckt: ☐

- Wenn Sie eine eigene Internet-Homepage betreiben, gelten die gleichen Vorsichtsmaßnahmen: E-Mail-Adressen auf Webseiten sind ein leichtes Ziel für Adressensammler! Auch hier gibt es einige einfach umzusetzende Tipps: Bauen Sie zusätzliche Leerzeichen in die Adresse ein, oder bilden Sie die Angaben nicht in Textform, sondern in einer Grafik ab.

Gecheckt: ☐

Leider gehen diese Maßnahmen zu Lasten der Bequemlichkeit: Automatisierte Mail-Verknüpfungen gibt es dann nicht mehr – aber das muss beim Schutz vor Spam und schädlicher Software manchmal in Kauf genommen werden!

Reaktion auf Spam-Mails

Sollte sich trotz aller technischen Schutzmaßnahmen eine Spam-Nachricht in Ihren Posteingang verirrt haben, können Sie durch eine Reihe einfacher Maßnahmen den „Schaden" minimieren:

- Aktivieren Sie immer die Sicherheitsoptionen für Ihr E-Mail-Programm. Dazu gehören Einstellungen wie die Anzeige von Nachrichten in reiner Textdarstellung oder das Ausblenden von Grafiken und Bildern. Auch wenn man sich in die Anfänge der Computertechnologie zurückversetzt fühlt – es dient Ihrer Sicherheit!

Gecheckt: ☐

- Seien Sie beim Blick in Ihren elektronischen Briefkasten grundsätzlich vorsichtig und misstrauisch! Jede Angabe vom Absendernamen über die Betreffzeile bis hin zum Dateinamen bei angehangenen Dateien kann gefälscht sein!

Gecheckt: ☐

- Löschen Sie die Nachricht ungeöffnet, wenn auf Grund des Absenders oder des Betreffs eindeutig ist, dass es sich um Spam handelt. Schon das Öffnen einer Nachricht kann schädliche Software übertragen oder ausführen. Denken Sie daran, dass der Absendername gefälscht sein kann!

Gecheckt: ☐

- Wenn Sie sich nicht sicher sind, ob es sich um eine Nachricht handelt, die Sie wirklich lesen möchten, sollten Sie zunächst alle Sicherheitseinstellungen Ihres E-Mail-Programms und den Virenschutz prüfen und so restriktiv wie möglich einstellen. Auch eine telefonische Nachfrage beim vermeintlichen Absender kann sinnvoll sein – insbesondere wenn die Nachricht unaufgefordert zugesendet wurde oder Dateianhänge enthalten sind. Weitere Anzeichen sind ungewöhnliche Uhrzeiten für den Mail-Versand oder das Verfassen in einer für den Absender ungewöhnlichen Sprache.

Gecheckt: ☐

- Antworten Sie niemals auf eine Spam-Mail – auch nicht aus Verärgerung oder mit der Bitte, keine Mails mehr an Sie zu versenden! Sie erreichen nichts mit dieser Vorgehensweise – außer dass der Spam-Versender nun die Bestätigung hat, dass Ihre E-Mail-Adresse echt und aktiv ist!

Gecheckt: ☐

- Auch die angebliche Möglichkeit, sich aus einer Verteilerliste auszutragen bzw. die zukünftige Mailzusendung zu unterbinden, ist nichts anderes als ein Trick der Spammer, um Sie zur Reaktion und damit zur Bestätigung der Mail-Adresse zu bewegen! Nur wenn Sie sich wirklich sicher sind, dass Sie sich in der Vergangenheit für einen Newsletter eingetragen haben, können Sie diesen Weg nutzen, um sich wieder auszutragen.

Gecheckt: ☐

Keine unfreiwillige Unterstützung für die Spammer

Es gibt viele Mittel und Wege, die sich die Spammer ausgedacht haben, um sich neue Adressen zu beschaffen:

- So gibt es beispielsweise viele Internet-Seiten, die anscheinend interessante Berichte, Witze oder Comics enthalten. Die dort vorhandene Benachrichtigungsmöglichkeit für Freunde und Kollegen dient in Wahrheit nur dazu, die Adressen zu sammeln und weiterzugeben. Wenn es sich wirklich lohnt, kopieren Sie lieber den Link der Webseite und schicken diese ganz normal per Mail weiter.

Gecheckt: ☐

Kein Spam – aber auch ärgerlich:

Eine besondere Form der unerwünschten Mails sind Kettenbriefe und Falschmeldungen – die so genannten „Hoaxes“:

- In Kettenbriefen wird oft an die Hilfsbereitschaft des Empfängers appelliert: Häufig geht es um die Hilfe für Katastrophenopfer, ein Erfolg versprechendes Gewinnspiel oder die angeblich so dringend benötigte Organspende für ein krankes Kind. Herzzerreißende Texte und Bilder ergänzen diese Nachrichten. Natürlich wird der Empfänger aufgefordert, diese Nachricht sofort an möglichst viele Mail-Empfänger weiterzuleiten. Leider steckt dahinter fast immer nur der Versuch, eine möglichst große Verbreitung für diesen „Scherz“ zu erreichen. Echte Hilfsorganisationen suchen niemals über Kettenbriefe Unterstützung!

  Gecheckt: ☐

- Der Begriff „Hoax“ umfasst Falschmeldungen, die vor allem im Zusammenhang mit Computerviren verbreitet werden. Diese Meldungen stammen angeblich von Virenschutzherstellern oder anderen wichtigen Computerunternehmen. Die User werden auf einen neuen Virus oder Wurm hingewiesen und dazu aufgefordert, die Warnung an möglichst viele Empfänger weiterzuleiten. In der Vergangenheit gab es schon Falschmeldungen, die den Anwender aufgefordert haben, bestimmte Dateien zu löschen – diese waren aber für den Betrieb des Computers wichtig! Man könnte also sogar sagen: Die Falschmeldung war eine Art Computervirus, der nur durch den User ausgeführt wurde!

  Gecheckt: ☐

Auch wenn es gut gemeint ist: Leiten Sie solche Kettenbriefe und Warnungen niemals weiter! Nur in den seltensten Fällen werden Sie dem Empfänger eine wichtige Information oder die Warnung vor einer realen Gefahr zukommen lassen.

Spam-Schutz im Netzwerk

In einem Netzwerk mit einem eigenen Mail-Server gibt es zusätzliche Möglichkeiten und Chancen, die Spam-Flut möglichst früh zu stoppen und so die Anwender zu entlasten. Aus Kosten- und auch aus Sicherheitsgründen sollte die Blockade von Spam-Mails zu einem möglichst frühen Zeitpunkt erfolgen. Bereits am Übergang vom Internet zum internen Netzwerk gibt es einige Ansatzpunkte:

- Aktuelle Firewalls sind in der Lage, den E-Mail-Datenverkehr nicht einfach nur passieren zu lassen, sondern auch einer genaueren Analyse zu unterziehen. Bei dieser Überprüfung könnten beispielsweise bestimmte Schlüsselwörter im Betreff einer Nachricht ausgefiltert werden.

  Gecheckt: ☐

- Die meisten Mail-Server können ähnlich wie die E-Mail-Programme am Arbeitsplatz mit Listen von erlaubten bzw. verbotenen Absendern arbeiten – allerdings gelten diese Einstellungen dann global für die gesamte Mail-Organisation. In der Praxis bedeutet das häufig einen unverhältnismäßig hohen Pflegeaufwand für die Administratoren. In bestimmten Situationen kann dies aber eine sinnvolle Ergänzung für andere Schutzmechanismen sein.

  Gecheckt: ☐

- Bei der Konfiguration der Mail-Server können ein paar einfache Tricks dazu beitragen, die Anzahl der Spam-Mails zu reduzieren. Prüfen Sie, ob bestimmte Standard-Mailverteiler wie beispielsweise „Info@“ oder „Einkauf@“ vom Internet aus erreichbar sein müssen. Einige Mail-Server unterstützen hier eine Beschränkung auf die rein interne Verwendung solcher Verteiler.

Gecheckt: ☐

- Prüfen Sie, welche Meldungen Ihr E-Mail-Server in das Internet zurücksendet, wenn Mail-Adressen nicht existieren oder nicht erreichbar sind. Zu viele Informationen können dem Spammer verraten, welche E-Mail-Adressen wirklich existieren und welche nicht. Diese Form des Ausspähens von Adressen erfolgt vollautomatisiert und wird auch als „Dictionary Attack“ bezeichnet.

Gecheckt: ☐

- Eine sehr wirkungsvolle Schutzmaßnahme ist die Verwendung von so genannten „DNS-Blacklists“. Diese Listen werden von kommerziellen wie nicht-kommerziellen Anbietern im Internet ständig aktualisiert und enthalten die Absenderangaben bekannter Spam-Versender. Trifft nun eine neue Mail an Ihrem Mail-Server ein, werden zunächst die Einträge auf der Blacklist überprüft. Findet sich dort die Absenderadresse, kann die Mail-Annahme verweigert werden. Viele Mail-Server unterstützen heute diese Technologie. Durch die Kombination mehrerer Blacklists lässt sich ein relativ hoher Wirkungsgrad erreichen. Gemeinsam mit anderen Schutztechniken lässt sich dadurch die Anzahl der Spam-Mails drastisch reduzieren.

Gecheckt: ☐

- Kommerzielle Anti-Spam-Produkte für Netzwerke kombinieren häufig verschiedene Schutztechnologien wie Blacklists, Wortlisten und Aufstellungen erlaubter Absender. Durch die Kombination unterschiedlicher Kriterien lassen sich so fast alle Spam-Mails bereits am Server blockieren oder zumindest eindeutig kennzeichnen.

Gecheckt: ☐

Sichere Transaktionen – Schutz vor Online-Betrügern. Die wichtigste Regel: Misstrauisch sein!

Der beste Schutz vor Online-Betrügern ist sicherlich eine ausgeprägte Skepsis! Durch vorsichtiges Verhalten und besonnenes Handeln können Sie viel erreichen – technische Schutzmaßnahmen sind aber eine sinnvolle Ergänzung.

Informieren Sie sich genau über die Sicherheitsmaßnahmen, die Ihr Online-Geschäftspartner anbietet, und welche Möglichkeiten Sie selber haben, indem Sie beispielsweise mit Ihren Kontendaten sorgfältig umgehen:

- Halten Sie alle Informationen, die mit Ihren Transaktionen zu tun haben, geheim. Dazu gehören alle Passwörter, PINs, TANs, Kreditkarteninformationen oder auch Kundennummern. Speichern Sie diese Informationen niemals auf Ihrem PC ab – auch wenn es etwas lästig ist, die Informationen immer wieder neu einzugeben.

Gecheckt: ☐

Checkliste: Schutz für Unternehmen

- Sprechen Sie mit Ihrer Bank und mit den Kreditkartenfirmen. Fragen Sie nach Tipps für die Online-Verwendung von Kartendaten. Prüfen Sie, wie hoch das Limit für Online-Überweisungen ist, und reduzieren Sie es, wenn Ihnen der Betrag zu hoch erscheint.

Gecheckt: ☐

- Passwörter sind ein schwieriger Themenbereich: Wenn Sie selber ein Passwort oder eine PIN generieren dürfen, sollten Sie unter keinen Umständen einfach zu erratende Wörter oder Zeichenfolgen wählen. Zu komplexe Zeichenfolgen mit Ziffern und Sonderzeichen wurden lange von Security-Experten empfohlen – führen aber oft zu dem berüchtigten Post-it-Zettel am Monitor! Je nach zulässiger Länge des Passworts können Sie sich evtl. einen Passwort-Satz ausdenken. Sind nur kurze Passwörter erlaubt, kann man sich ein Passwort aus den Anfangsbuchstaben des Passwort-Satzes bilden. Andernfalls können auch Ziffernfolgen hilfreich sein, wenn Sie sie aus dem Kopf ableiten können – also z. B. „mein Geburtsdatum plus meine Postleitzahl".

Gecheckt: ☐

- Informieren Sie sich bei Ihrer Bank, welche modernen Sicherheitsstandards unterstützt werden. Aktuelle Onlinebanking-Anwendungen können z. B. für einige Euro Zusatzkosten mit einem Chipkartenleser ausgestattet werden. Damit sind Sie in der Lage, Ihre Transaktionen mit Ihrer EC-Karte oder einer anderen Kundenkarte abzusichern. Diese Technologie wird als HBCI bezeichnet und gilt als sehr sicher.

Gecheckt: ☐

- Senden Sie niemals E-Mails, in denen diese Informationen enthalten sind. Unverschlüsselte E-Mails können von jedermann gelesen werden.

Gecheckt: ☐

- Mitarbeiter von Internet-Providern, Banken, Online-Shops, Auktionshäusern usw. dürfen Sie nie nach Daten oder sogar Benutzerinformationen fragen – weder per E-Mail noch am Telefon. Geben Sie daher niemals Auskunft, und informieren Sie Ihren Geschäftspartner umgehend, wenn sich solche E-Mails im Posteingang finden. Sie können so dazu beitragen, andere Anwender zu warnen!

Gecheckt: ☐

- Wenn Ihnen andere Dinge merkwürdig vorkommen – hat sich z. B. das Design der Online-banking-Webseite verändert, kontaktieren Sie ihren Geschäftspartner, bevor Sie irgendwelche Transaktionen durchführen.

Gecheckt: ☐

- Geben Sie die Web-Adresse (URL) Ihres Partners immer manuell ein, oder nutzen Sie einen abgespeicherten Favoriten des Internet-Browsers. In letzter Zeit haben sich Fälle gehäuft, in denen Anwender mit einer täuschend echt aussehenden E-Mails auf eine gefälschte Webseite gelockt wurden, um dort Kontendaten und Passwörter (Phishing) einzugeben. Mit den eingegebenen Informationen konnten die Online-Betrüger großen Schaden anrichten.

Gecheckt: ☐

Checkliste: Schutz für Unternehmen

- Wenn Sie eine Webseite verlassen, sollten Sie sich immer explizit abmelden und alle Browser-Fenster schließen. Sonst ist es einem Betrüger unter Umständen möglich, die Sitzung ohne Ihr Wissen weiterzuführen.

Gecheckt: ☐

- Nutzen Sie nach Möglichkeit keine öffentlich zugänglichen Internet-Arbeitsplätze, wie z. B. in Internet-Cafés, für Transaktionen. Kleine Spionageprogramme sind in der Lage, Ihre Tastatureingaben aufzuzeichnen und an unbefugte Personen weiterzugeben. Lässt sich dies nicht vermeiden, sollten Sie zumindest alle anderen Vorsichtsmaßnahmen beachten und zusätzlich nach der Beendigung einer Sitzung in den Optionen des Internet-Browsers den Verlauf (History) und die zwischengespeicherten Dateien (Cache) löschen.

Gecheckt: ☐

- Speziell bei Online-Auktionen und Bestellungen im Internet können Treuhand-Dienste ein guter Schutz vor Betrügern sein. Sie nehmen sozusagen eine neutrale Position zwischen Verkäufer und Käufer ein und leiten eine Zahlung nur dann weiter, wenn die Ware in einem ordnungsgemäßen Zustand beim Empfänger angekommen ist. Insbesondere bei internationalen Geschäften sind diese Dienstleister eine große Hilfe.

Gecheckt: ☐

Auch wichtig: die Technik

Neben den Verhaltenstipps gibt es noch eine Reihe von Empfehlungen für die Einstellungen des Internet-Browsers und die Konfiguration Ihres Systems. Bedenken Sie aber, dass dies alles nicht hilft, wenn Sie beispielsweise einer unbefugten Person Ihre Kontendaten am Telefon mitteilen. Bei der Bedrohung durch den Online-Betrüger steht der Mensch im Mittelpunkt!

- Um es dem Online-Betrüger schwieriger zu machen, Spionage-Programme in Ihren Rechner einzuschleusen, sollten Sie die gleichen grundlegenden Sicherheitsmaßnahmen beachten, die für den Schutz vor Hackern gelten.

Gecheckt: ☐

- Aktualisieren Sie Ihr Betriebssystem, den Internet-Browser und die Onlinebanking-Anwendung regelmäßig, und prüfen Sie auf den Internet-Seiten der Hersteller, ob es besondere Sicherheitsempfehlungen gibt!

Gecheckt: ☐

- Setzen Sie ein aktuelles Virenschutzprogramm ein. Viren, Würmer & Co. haben oft Ihre Passwörter oder Kontendaten im Visier!

Gecheckt: ☐

- Benutzen Sie eine Personal Firewall! Dieser persönliche Schutzwall um Ihren PC verringert die Gefahr, dass unberechtigte Personen ohne Ihr Wissen Zugriff auf vertrauliche Informationen haben oder schädliche Software auf Ihren PC übertragen.

Gecheckt: ☐

Checkliste: Schutz für Unternehmen

- Schalten Sie in Ihrem Internet-Browser die so genannten aktiven Inhalte (ActiveX, Java-Applets) aus, oder stellen Sie zumindest die Option zur Anzeige einer Eingaubeaufforderung ein. Aktive Komponenten können zur Anzeige von Eingabeaufforderungen genutzt werden sowie wichtige Bildschirminhalte verdecken oder durch gefälschte Informationen überschreiben.

Gecheckt: ☐

- Prüfen Sie bei der Übertragung wichtiger Informationen die Adresszeile des Internet-Browsers: Statt mit „http" sollte die Internetadresse immer mit „https" beginnen. Dies bedeutet, dass die Übertragung der Informationen verschlüsselt wird. Die meisten Internet-Browser zeigen in diesem Fall noch zusätzlich ein Symbol in Form eines Vorhängeschlosses an. Übertragen Sie niemals wichtige Informationen wie Kreditkartendaten, wenn die Übertragung nicht per https abgesichert ist. Dies gilt auch für scheinbar harmlose Webseiten, da die übertragenen Informationen ohne großen Aufwand ausgespäht werden können.

Gecheckt: ☐

- Um eine verschlüsselte Übertragung zu ermöglichen, sind auf den Seiten des Anbieters der Webseite so genannte Zertifikate erforderlich. Als Besucher der Webseite können Sie sich die Detailinformationen zu dem Zertifikat anzeigen lassen, um beispielsweise zu prüfen, für wen es ausgestellt wurde und ob es gültig ist. Wie diese Überprüfung stattfindet und was die Fehlermeldungen zu Zertifikaten bedeuten, erfahren Sie in der Hilfefunktion des Internet-Browsers. Sollten beim Aufruf einer Webseite, die in der Vergangenheit keine Probleme bereitet hat, Fehlermeldungen angezeigt werden, die mit dem Zertifikat zu tun haben, sollten Sie den Vorgang umgehend abbrechen und sich mit Ihrem Geschäftspartner in Verbindung setzen.

Gecheckt: ☐

Gewaltverherrlichung, Pornografie, Volksverhetzung – die Schattenseite des Internets

Online-Müll korrekt entsorgt

Auch in Unternehmensnetzwerken tauchen immer mehr Inhalte auf, die mit einer sinnvollen Verwendung des Internets nichts zu tun haben.

Online-Schmutzfinken verwenden die unterschiedlichsten Tricks und Kniffe, um Sie auf Ihre Seiten zu locken. Unverfängliche E-Mails oder angebliche Gewinnspiele sind nur zwei Beispiele für den riesigen Aufwand, den diese Herrschaften treiben.

- Landen Sie versehentlich auf einer dieser Seiten, sollten Sie das Fenster Ihres Internet-Browsers sofort schließen. Bestätigen Sie keine Schaltflächen oder Dialogboxen, sondern nutzen Sie das Symbol, das in Ihrer grafischen Benutzeroberfläche zum Schließen eines Fensters vorgesehen ist (bei Microsoft Windows das Kreuz in der rechten oberen Ecke des Fensters).

Gecheckt: ☐

- Sollten Sie eine E-Mail bekommen haben, die Sie auf diese Seite gelockt hat, lohnt es sich nicht,darauf zu antworten, um sich zu beschweren – löschen Sie sie stattdessen.

Gecheckt: ☐

- Zögern Sie nicht, die Seiten bei der Polizei oder anderen Institutionen wie www.jugendschutz.net zu melden, wenn Sie der Meinung sind, dass Sie illegale Inhalte (z. B. Kinderpornografie oder rechtsradikale Inhalte) gefunden haben.

Gecheckt: ☐

- Die hier beschriebenen Inhalte und Spam-Mails gehören eng zusammen. Sie sollten also die gleichen Vorsichtsmaßnahmen beachten, die wir im Bereich Schutz vor Spammer für Sie zusammengestellt haben!

Gecheckt: ☐

Technik – die Grundlagen

Neben Tipps zum Schutz vor den „speziellen Inhalten der Internet-Schmutzfinken" gelten auch hier die gleichen Grundregeln für Ihre PC-Sicherheit! Insbesondere Seiten mit jugendgefährdenden Inhalten werden oft dazu missbraucht, Viren, Trojaner oder Dialer auf die Rechner der Besucher zu übertragen. Seien Sie daher immer wachsam! Eine wesentliche Verbesserung der Sicherheit erreichen Sie bereits, wenn Sie drei wichtige Tipps beherzigen:

- Aktualisieren Sie Ihr Betriebssystem, den Internet-Browser und die wichtigsten Anwendungsprogramme regelmäßig, und prüfen Sie auf den Internet-Seiten der Hersteller, ob es besondere Sicherheitsempfehlungen gibt!

Gecheckt: ☐

- Setzen Sie ein aktuelles Virenschutzprogramm ein, und sorgen Sie für regelmäßige Updates!

Gecheckt: ☐

- Benutzen Sie eine Personal Firewall! Dieser persönliche Schutzwall um Ihren PC verringert die Gefahr, dass unberechtigte Personen ohne Ihr Wissen Zugriff auf vertrauliche Informationen haben oder schädliche Software auf Ihren PC übertragen.

Gecheckt: ☐

Technik – für Fortgeschrittene

Schon vor einigen Jahren hat die Software-Industrie damit begonnen, Schutzfunktionen gegen unerwünschte Inhalte zu entwickeln. Dies ist eine technologische Herausforderung, da die Inhalte nicht immer einfach zu identifizieren sind: In einen völlig harmlosen Text kann beispielsweise ein gewaltverherrlichendes Foto eingebettet werden.

Die meisten Filtersysteme haben daher auch heute noch eine recht hohe Fehlerquote und schaffen es nicht, die unerwünschten Inhalte gänzlich auszufiltern. Filter können Ihnen aber einen großen Teil der Arbeit abnehmen!

- Einige Software-Unternehmen haben den von ihnen hergestellten Internet-Browser mit speziellen Filterfunktionen ausgestattet. Oft werden diese Filter als „Inhaltsratgeber", „Inhaltsfilter" oder

Checkliste: Schutz für Unternehmen

„Contentfilter“ bezeichnet. Ob Ihr Internet-Browser mit einer solchen Funktion ausgestattet ist, können Sie in der Produktdokumentation oder in der Online-Hilfe nachlesen. Diese Filter können meistens über die Einstellungen oder Optionen des Browsers eingeschaltet und konfiguriert werden.

Gecheckt: ☐

- Viele Router, die eingesetzt werden, um per ISDN oder DSL eine Verbindung ins Internet aufzubauen, sind mittlerweile mit Filtermöglichkeiten ausgestattet worden. In der Regel basieren diese elektronischen Wächter auf Stichwörtern, die in der Webadresse – der so genannten URL – enthalten sind und nicht auf den tatsächlichen Seiteninhalten. Auch hierfür finden sich weiterführende Informationen in der Dokumentation für diese Geräte.

Gecheckt: ☐

- Einige Internet-Provider bieten speziell gesicherte Zugänge an. Setzen Sie sich dazu mit Ihrem Internet-Anbieter in Verbindung und prüfen Sie, ob solche Angebote für Ihren Internet-Zugang verfügbar sind und was sie leisten.

Gecheckt: ☐

- Am Software-Markt werden einige kommerzielle Lösungen für das Filtern von Mail- und Web-Inhalten angeboten. Diese Software wird sowohl für einzelne PCs als auch für komplette Netzwerke mit zentralem Internet-Zugang angeboten.

Gecheckt: ☐

- Viele dieser Internet-Seiten versuchen, so genannte „Dialer“ zu installieren. Diese Einwählprogramme manipulieren ohne Wissen des Anwenders die Konfiguration des PC und ersetzen die bisherige Internet-Verbindung durch extrem teure Einwahlnummern. Durch Dialer können astronomisch hohe Telefonrechnungen entstehen! Daher sollten Sie bei Ihrem Telekommunikationsanbieter unbedingt kostenpflichtige Sonderrufnummern (z. B. 0190, 0900 usw.) sperren lassen.

Gecheckt: ☐

Gecheckt? Geschafft!

Sie haben alle wichtigen sicherheitsrelevanten Bereiche geprüft und die empfohlenen Maßnahmen angewendet. Damit haben Sie einen entscheidenden Beitrag für Ihren optimalen Online-Schutz geleistet.