

IT AN DER UNIVERSITÄT ZU KÖLN



Thema: Der sichere Computer plus...

Der sichere Windows-Computer | Seite 2

Datenspione im öffentlichen Netz | Seite 3

Virenschutz | Seite 3

Datensicherung | Seite 4

Sie finden unsere IT-Beilage auch als PDF im Internet unter <http://ukoeln.de/98Y96>



Interview mit LL.M. Alexander May, Datenschutzbeauftragter der Universität zu Köln

Der technikbegeisterte Jurist Alexander May hat die Funktion des Datenschutzbeauftragten der Universität zu Köln. Aufgabe des Datenschutzbeauftragten ist es, die Universitätsverwaltung bei der Umsetzung des Datenschutzes zu unterstützen und als Ansprechpartner für Studierende und Mitarbeiter Fragen des Datenschutzes zu klären.

Herr May, wie ist eigentlich Ihr eigener Computer geschützt?

Alexander May: Ich habe im Büro einen Standard-Verwaltungscomputer. Für alle Passwortzugänge habe ich je ein eigenes Passwort, das den Regeln der Verwaltung entspricht: mindestens acht Zeichen, davon mindestens eine Ziffer und mindestens ein Buchstabe, insgesamt nicht sprechend. Ich bilde die Passwörter nach einer abstrakten Regel, weil sie dann leichter zu merken sind. Beim Verlassen des Raumes aktiviere ich die passwortgeschützte Bildschirmsperre. Meine Datenschützerdateien lege ich in einem geschützten Bereich ab, auf den nur ich Zugriff habe und der täglich gesichert wird. Es läuft eine aktuelle Virenschutzsoftware und der Computer befindet sich hinter der Verwaltungs-Firewall. Ich öffne verdächtige Anhänge nicht (auch keine „Spaß-Präsentationen“) und

klicke nicht auf jeden dubiosen Link. Ein wenig Aufmerksamkeit bei der Computer-Nutzung gehört schon dazu. Trotzdem weiß ich, dass bei aller Sorgfalt ein Computer beim Surfen auch „im Vorbeigehen“ infiziert werden kann und vertraue darauf, dass es dann jemandem auffällt. Ich habe das Gefühl, in der Verwaltung von einer aufmerksamen IT-Organisation „behütet“ zu sein, weiß aber auch, dass ich – wie jeder andere Nutzer auch – durch ein wenig Umsicht meinen Beitrag zur IT-Sicherheit leisten muss. Zuhause handhabe ich es mit meinem privaten Computer ähnlich.

Welche Pflichten haben Mitarbeiter beim Schutz ihres Dienstcomputers, zum Beispiel beim Einsatz von Virenschutzprogrammen und so weiter?

AM: Für die Verwaltung sind die Pflichten der Beschäftigten in einer Dienstvereinbarung geregelt. Darin ist im Wesentlichen aber nur das niedergelegt, was ohnehin gilt:

Der Arbeitsplatz-Computer ist ein dienstliches Arbeitsmittel. Der Dienstcomputer ist so einzusetzen, wie der Fachvorgesetzte es vorgibt. Das bedeutet aber auch, dass den Vorgesetzten eine Organisationspflicht trifft: Die Beschäftigten müssen geschult und angewiesen

werden und die Technik muss so organisiert sein, dass sie für den dienstlichen Einsatz geeignet ist. Dazu gehört es auch für Virenschutz, Datensicherung, Support, Wartung und so weiter zu sorgen. Wenn der Vorgesetzte das nicht kann, muss er das Problem in der Organisation lösen lassen.

Die Pflicht der Beschäftigten ist es, sich schulen zu lassen und die vorgegebenen Sicherheitsregeln anzuwenden. Zum Beispiel: Passwortregeln anwenden, Vertraulichkeit wahren, Virenschutz aktuell halten, Updates einspielen, Räume abschließen und – wichtig! – den Verdacht auf technische Probleme dem Vorgesetzten/der Technikabteilung melden!

IT-Sicherheit ist, wie es so schön heißt, eine Gesamtaufgabe der Dienststelle. Jeder Teil der Organisation hat darin eine Aufgabe, jeder muss seinen Teil dazu beitragen und niemand kann alle Verantwortung von sich weisen oder sie insgesamt nur einer Stelle zuschieben.

Welche Pflichten haben Mitarbeiter in Bezug auf Datensicherung? Muss ich eine Datensicherung machen und wenn ja, wo?

AM: Noch einmal: Die Organisation der Datensicherung obliegt demjenigen, der den Einsatz von IT angeordnet hat. Er ist verantwortlich für den sicheren Einsatz der IT einschließlich der Pflicht, Daten vertraulich, integer und verfügbar zu halten. Teil dessen ist die Datensicherung, die genauso Vertraulichkeit gewährleisten muss, wie das zu sichernde System. Das Sicherungsintervall hängt von vom Schutzbedarf der Daten ab. In bestimmten Bereichen wird täglich zu sichern sein, in anderen wöchentlich. In der

Regel wird auf Netzlaufwerke und Bänder gesichert. Wir haben aber auch in einem Fall einen Tresor angeschafft, in dem nun Festplatten liegen.

Müssen die Angebote der Universität zu Köln beziehungsweise des RRZK genutzt werden oder können Mitarbeiter ihre eigene Software verwenden? Darf ich zum Beispiel andere Virenschutzprogramme als Sophos installieren, weil ich Sophos nicht mag?

AM: Die Mitarbeiter können das nur frei entscheiden, wenn es ihnen erlaubt ist. In der Verwaltung ist die Beschaffung und Installation von Software nur mit Erlaubnis der IT-Abteilung zulässig. In den Fakultäten und Lehrstühlen ist die Handhabung unterschiedlich. Die Auswahl der eingesetzten Software (einschließlich Virenschutz) ist aus verschiedensten Gründen eine Angelegenheit der Dienststelle (zum Beispiel Sicherheit, Funktionalität, Schulung, Lizenzen, Kosten) und ich halte es für verfehlt, die Entscheidung darüber ausschließlich den Beschäftigten zu überlassen.

Welche Konsequenzen haben Mitarbeiter zu befürchten, die ihren Pflichten in diesen Punkten nicht nachkommen?

AM: Meine Pflicht als Beschäftigter ist es, die dienstlichen Arbeitsmittel bestimmungsgemäß und weisungsgemäß zu verwenden. Wenn es keine konkrete Weisung gibt, muss ich auf das Defizit hinweisen, um Weisung/Erlaubnis bitten oder eine fragliche Nutzung unterlassen. Mit anderen Worten: bloß weil etwas nicht ausdrücklich verboten wurde, ist es nicht automatisch erlaubt! Das Bundesarbeits-

Editorial

Liebe Virenschützer,

wir alle wissen, wie wichtig es ist auf dem aktuellen Sicherheitsstand zu sein. Und dennoch haben wir alle ein schlechtes Gewissen, denn die Sicherheit des eigenen Computers rutscht auf der ToDo-Liste schnell nach unten.

Ist der Virensch scanner auf dem aktuellen Stand? Wann haben wir eigentlich das letzte Backup durchgeführt? Sind alle Updates installiert? War die E-Mail gestern ernst gemeint oder ein Phishingversuch? Wie kann ich es verhindern, mich täglich durch diese Mengen an Spam kämpfen zu müssen? Wie sicher ist eigentlich surfen im Café mit kostenfreiem WLAN-Zugang? Wer kann sich schon diese komplizierten Passwörter für alle Accounts merken, die man verwenden muss?

Fragen, die uns ständig durch den Kopf schwirren. Und trotzdem gehört für die Meisten von uns die Sicherheit des eigenen Computers nicht zur Routine, sondern zu den lästigen Dingen, die getan werden müssen. Theoretisch ist uns ja allen klar, dass Unbedachtheit Risiken birgt, aber „et hät noch immer joot jejeange“. Warum sollte sich das auf einmal ändern? Wenn sich dann aber doch ein Schädling eingenistet hat oder Nutzerdaten geklaut wurden, ist es zu spät. Und guter Rat meist sehr teuer. Und damit sind wir schon beim nächsten Satz des Kölschen Grundgesetzes: „Wat fott es, es fott“. Ärgerlich, aber nicht mehr zu ändern.

In dieser IT-Beilage haben wir einige wichtige Bausteine zur Sicherheit Ihrer Computer zusammengetragen, um grundlegende Informationen und hilfreiche Tipps zu geben. Und vielleicht fühlen wir und unsere Viren uns alle danach ein klein wenig besser auf unseren Computern geschützt.

Ingeborg Wöhr
Marc Seifert

Ingeborg Wöhr und Marc Seifert

PS: Als kleine Lektüre zum Weiterlesen empfehlen wir Ihnen die c't Ausgabe 20/2011 sowie das Sophos Schreckxiikon, zu finden im Web unter <http://bit.ly/oXCFdj>



Rubriken

Newsfeed 2
Computerkurse 4

gericht hat mehrfach Kündigungen wegen privater Internetnutzung bestätigt, obwohl vom Arbeitgeber kein ausdrückliches Verbot ausgesprochen war. Der Grund ist, dass Arbeitszeitbetrug oder strafbare beziehungsweise den Ruf des Arbeitgebers schädigende Nutzung (etwa aufrufen/verschicken extremistischer/pornografischer Dateien) per se verboten sind.

Die Folgen sind die üblichen

arbeits-/dienstrechtlichen Sanktionen, die – kurz gesagt – vom ermahnenen Gespräch über die Abmahnung bis zur fristlosen Kündigung reichen. Gegebenenfalls ist auch der Personalrat zu beteiligen. Wichtig: Für jeden Einzelfall muss jeweils eine verhältnismäßige Maßnahme gefunden werden, so dass pauschale Aussagen nicht möglich sind. Niemand muss also wegen einer einzigen harmlosen privaten

E-Mail Angst vor einer Kündigung haben. Aber ein Dienst-Computer mit Internetanschluss ist eben auch kein Freifahrtschein für eine Spritztour ohne Navi und Anschnallgurt auf dem „Information Highway“.

Herr May, vielen Dank für die Beantwortung unserer Fragen.

■ Interview: Marc Seifert, Ingeborg Wöhr

Der sichere Windows-Computer



Grundsätzlich gilt: den sicheren Computer gibt es nicht. Bei dem derzeitigen Aufkommen an Schädlingen und kriminellen Angriffen auf Computer erscheint es nahezu unmöglich, einen Computer absolut sicher und frei von Bedrohungen zu halten. Häufig verwendete Programme, wie zum Beispiel Windows, Microsoft Office, Adobe Acrobat und alle gängigen Browser sind durchweg einer hohen Bedrohung ausgesetzt. Aber: Sie können es den Angreifern erschweren, Ihren Computer zu übernehmen, Ihre Daten zu missbrauchen und Sie zu schädigen. So wie Sie Fenster schließen, die Eingangstür abschließen und nicht jeden Fremden in Ihre Wohnung lassen, so gibt es auch für Ihren Windows-Computer ein paar einfache Richtlinien und Hilfsmittel, wie Sie das Risiko deutlich minimieren können. Dieser sowie die weiteren Artikel unserer IT-Beilage liefern Ihnen dazu die nötige Hilfestellung. Und das Beste daran: Sie brauchen noch nicht einmal den technischen Hintergrund zu verstehen, wenn Sie sich dafür nicht interessieren.

Ihr wichtigstes Hilfsmittel ist Ihr gesunder Menschenverstand. Wenn Sie kein Paket erwarten, dann ist es auch relativ unwahrscheinlich, dass Ihnen ein Paketlieferdienst eine E-Mail in englischer Sprache schickt und Sie auffordert, Ihre Bankverbindung nebst PIN anzugeben. Auch vom RRZK werden Sie keine E-Mail erhalten mit der Bitte, Ihr Webmail-Passwort anzugeben, weil Ihr Postfach voll ist. Wenn Ihr Postfach voll wäre, wie hätten wir Ihnen dann diese E-Mail zustellen sollen? Klicken Sie nicht einfach auf jeden Link, öffnen Sie ausschließlich E-Mails, wenn Ihnen diese vertrauensvoll vorkommen und handeln Sie bei der Arbeit mit Ihrem Computer mit eben so viel Bedacht und Umsicht wie im Straßenverkehr. Damit schützen Sie sich und andere.

Sie können Ihren gesunden Menschenverstand übrigens unterstützen, indem Sie die Funktion „Automatische Dateinamenerweiterung ausblenden“ deaktivieren (Windows Explorer öffnen: Linke Maustaste auf Start > einen beliebigen Ordner anklicken > Organisieren (links oben unter Datei) > Ordner- und Suchoptionen > Ansicht > unter Erweiterte Einstel-

lungen das Häkchen bei „Erweiterungen bei bekannten Dateitypen ausblenden“ entfernen). Hat Windows vorher nur den Dateinamen „Antragsformular“ angezeigt, wird daraus jetzt „Antragsformular.pdf“. Die schädliche Mail mit dem Anhang „Antragsformular.pdf“ wird jetzt als „Antragsformular.pdf.exe“ angezeigt und von Ihnen sofort als gefährlich erkannt.

Nur ein System auf dem aktuellen Stand kann sicher sein (siehe weiterer Artikel in dieser Ausgabe „Aktualität bedeutet Sicherheit“). Aktivieren Sie unbedingt die Windows Update Funktion (Start > Systemsteuerung > Windows Update), die automatisch dafür sorgt, dass Ihr Windows und die anderen Microsoft Programme immer auf dem aktuellen Stand bleiben. Für alle anderen Programme müssen Sie sich darum leider meist selbst kümmern. Viele Programme bieten die Möglichkeit, automatisch nach Aktualisierungen zu suchen beziehungsweise diese zu installieren, was Sie dann auch regelmäßig und möglichst häufig in Anspruch nehmen sollten. Bei Software, die diese Option nicht bietet, bleibt nur der mühsame – aber im Sinne Ihrer eigenen Sicherheit – lohnenswerte Weg, selbst regelmäßig nach aktuellen Versionen zu suchen.

Virenschutz gehört heute zur Standardausstattung jedes Computers (siehe weiterer Artikel in dieser Ausgabe „Virenschutz“). Die Universität zu Köln stellt allen Angehörigen kostenlos das Programm Sophos zur Verfügung. Auf der entsprechenden Webseite gibt es eine Kurzanleitung und ein Video zur Installation. Virens Scanner sollten mindestens einmal pro Stunde aktualisiert werden. Das ist bei der Sophos Version, die Sie über das RRZK erhalten bereits voreingestellt.

Obwohl aktuelle Virenschutzprogramme vor vielerlei Arten von Schädlingen schützen, möchten manche Nutzer Ihre Sicherheit nicht allein einem Produkt eines Herstellers anvertrauen. Da die Installation von zwei oder mehr unterschiedlichen Virenschutzprogrammen im Zweifel böse Folgen, wie zum Beispiel hohe Einbußen an Rechenleistung für den Computer haben kann, kommen dabei oft Zusatzprogramme zum Einsatz, die den Einfall von Würmern, Trojanern et cetera verhindern sollen. Windows-

Nutzer können dabei auf Bordmittel von Windows zurückgreifen. Der Windows Defender schützt vor und reinigt bei Schadprogrammen (Aktivierung über Start -> Systemsteuerung -> Windows Defender). Unter Extras -> Optionen kann man die Automatische Überprüfung einstellen (einmal pro Woche reicht meist aus). Alternativprogramme wären zum Beispiel Spybot oder Adaware, die aber meist nicht so perfekt mit Windows harmonieren.

Die Windows Firewall sichert den Computer gegen unerwünschte Zugriffe aus dem Netz. Wenn Sie nicht zufällig Spezialist für Firewalls sind, lassen Sie die Finger von allen anderen Produkten und aktivieren Sie einfach die Windows Firewall (Start > Systemsteuerung > Windows Firewall). Ähnlich wie bei Sophos Antivirus und dem Windows Defender läuft auch dieser Dienst im Hintergrund und Sie müssen sich im Idealfall darum schon mal nicht mehr kümmern.

Für den Fall, dass doch mal etwas schief geht, hilft Ihnen die Beratung des RRZK gerne weiter. Die ideale Lösung ist natürlich immer, das komplette System neu aufzusetzen. Nur hat man dafür selten die Zeit. Sie können sich aber auf den Ernstfall vorbereiten. Mal ehrlich, so wie Sie eine Haftpflichtversicherung für Ihr Auto abschließen, so können Sie auch Ihr System versichern (unter Start > Systemsteuerung > Sichern und Wiederherstellen > Systemabbild erstellen). Sichern Sie regelmäßig ihr komplettes System auf eine externe Festplatte und bewahren Sie neben dem aktuellsten auch die Abbilder der letzten Sicherungen auf. Dann können Sie bei einer Infektion Ihres Computers mit Schadsoftware einfach ein älteres Abbild wieder einspielen und haben innerhalb von kurzer Zeit wieder exakt das System, wie Sie es vor der Infektion verwendet haben. Wenn Sie zusätzlich noch eine tägliche Datensicherung (siehe weiterer Artikel in dieser Ausgabe „Datensicherung leicht gemacht“) durchführen, haben Sie kaum Zeit verloren und können schnell dort weitermachen, wo Sie durch die Schädlinge unterbrochen wurden.

■ Marc Seifert
<http://ukoeln.de/2LLMN>

Newsfeed

Neuer Software Shop ab November 2011

Im Oktober 2011 wird das Regionale Rechenzentrum der Universität zu Köln den Verkauf von Softwarelizenzen auf ein neues System umstellen. Es steht Ihnen dann ein komfortabler Online Shop zur Verfügung, über den Sie nahezu alle Softwareprodukte einfach und schnell bestellen können. Alle bisherigen Bestellwege (Asknet Shop, E-Mail, Bestellformular, Kauf in der Berrenrather Straße et cetera) entfallen damit. Mit dem neuen Shop werden wir auch die Lizenzbedingungen für viele Produkte aktualisieren. Bitte informieren Sie sich gegebenenfalls rechtzeitig über Preise und Einsatzmöglichkeiten der von Ihnen genutzten Produkte, zum Beispiel über unser Kontaktformular. Bitte beachten Sie, dass für die Anmeldung zum neuen Software Shop ein Account der Universität zu Köln (Uni- oder S-Mail-Account) nötig sein wird. Ohne entsprechenden Account wird in Zukunft der Einkauf von Softwarelizenzen über die Universität zu Köln leider nicht mehr möglich sein. Bitte tragen Sie rechtzeitig dafür Sorge, dass alle Kolleginnen und Kollegen, die mit dem Einkauf und der Betreuung von Softwarelizenzen in Ihrer Einrichtung beschäftigt sind, über entsprechende Accounts verfügen. Informieren Sie bitte gegebenenfalls auch Ihre Promotionsstudierenden darüber, dass der Einkauf von Softwarelizenzen für nicht immatrikulierte Studierende dann nicht mehr möglich sein wird. <http://ukoeln.de/DMQRN>



Microsoft Landeslizenz NRW an der Universität zu Köln

Zum 01.07.2011 ist die Universität zu Köln der Microsoft Landeslizenz NRW (Microsoft Campus Agreement) beigetreten. Dies ermöglicht den flächendeckenden und kostengünstigen Einsatz von aktueller Microsoft Software (Windows und Office) auf dem gesamten Campus. Etwa ab November werden wir im Rahmen des neuen Software Shops der Universität zu Köln auch mit der Verteilung der Microsoft Produkte beginnen. Im Rahmen des Campus Agreement stehen allen Einrichtungen der Universität zu Köln folgende Produkte kostenfrei zur Verfügung:

- Microsoft Windows (Upgrade)
- Microsoft Office
- Core Client Access Lizenz



Grundsätzlich erhalten Sie im Rahmen des Campus Agreements stets die höchste Softwareversion (aktuell Windows 7 Enterprise und Office 2010 Professional Plus). Darüber hinaus gibt es ein Downgrade Recht, das es Ihnen ermöglicht, bei Bedarf auch andere Versionen (zum Beispiel Windows XP) einzusetzen. Es handelt sich um eine Mietlizenz, die jährlich von der Universität zu Köln verlängert wird. Der Vertrag wurde über unseren Handelspartner asknet AG abgewickelt und bereits von Microsoft akzeptiert. Aktuell bereiten wir die technischen und organisatorischen Voraussetzungen für die Implementierung der Software vor. Wichtigste Änderung wird die Aktivierung der Software sein. Diese erfolgt nicht mehr wie bisher über individuelle Aktivierungsschlüssel sondern selbstständig durch die Software über das Netzwerk der Universität zu Köln (von außerhalb über VPN) gegenüber einem KMS-Server.

Nachdem die Testphase sowie die Inbetriebnahme unseres neuen Software Shops abgeschlossen sind, gehen wir derzeit davon aus, die Software etwa ab November über den neuen Software Shop verteilen zu können. Umfassende Informationen dazu erhalten Sie von uns rechtzeitig vor dem Start der Softwareverteilung. Wir bitten Sie daher, aktuell vom Kauf der genannten Microsoft Produkte abzusehen beziehungsweise falls irgend möglich, die Ausstattung Ihrer Computer mit Windows und Office auf November zu verschieben. Weitere Informationen finden Sie auf unseren Webseiten. Dort finden Sie in Kürze auch weitere Dokumente mit den exakten Lizenzbedingungen, umfassenden Leistungsbeschreibungen sowie Empfehlungen zur Lizenzverwaltung. Außerdem steht Ihnen dort unser Kontaktformular für Rückfragen zur Verfügung. Bitte sprechen Sie uns für eine ausführliche Beratung an. <http://ukoeln.de/5KD4C>

2. cologne IT summit_ am 14. November 2011 in Köln

Kongress für Deutschlands zweitgrößtes ITK-Cluster
Mit der Veranstaltung soll die regionale ITK-Wirtschaft gefördert werden. Zusätzlich sollen Innovationsimpulse das Image und die Bedeutung der Region nachhaltig verbessern helfen. Darüber hinaus will der cologne IT summit_ als Alternative zu den großen überregionalen Plattformen insbesondere dem Mittelstand kostengünstigere Präsentationsmöglichkeiten anbieten.
Themen 2011: Smart-IT, Cloud, Mobility & Ubiquity, IT-Security 2.0, IT-Start-Ups, Standort-Entwicklung.
Veranstalter: Stadt Köln und Industrie- und Handelskammer zu Köln
<http://www.cologne-it-summit.de/>





Datenspione im öffentlichen Netz

Virtual Private Network (VPN) schützt vor Datenklau in ungeschützten Funknetzen

Das Internet gehört für die meisten von uns zum Alltag dazu. Im gewohnten Lebensablauf nutzen wir es, um uns zu informieren, mit anderen zu kommunizieren, Daten auszutauschen und zu publizieren. Verständlich, dass wir auf Reisen nur schwer darauf verzichten können. Umso praktischer ist, dass Hotels, Cafés und Fast-Food-Ketten kostenlos Wireless Local Area Network (WLAN) anbieten. Welche

Risiken diese öffentlichen Netze beherbergen, ist den Benutzern oft nicht bewusst.

Unverschlüsselte WLAN werden meistens der Einfachheit halber angeboten. Der Betreiber des Netzes möchte und kann oft nicht dafür sorgen, dass jeder Kunde mit einer bestimmten WLAN-Verschlüsselung zurechtkommt. Zu unterschiedlich sind die Konfigurationsschritte auf den verschiedenen Betriebssystemen und unendlich die Möglichkeiten das WLAN falsch einzurichten.

Ein unverschlüsseltes WLAN bedeutet aber auch, dass mit einfachen Hilfsmitteln jeder den Netzverkehr des Anderen mitlesen kann. Je nach Nutzungsverhalten erhält ein Angreifer nicht nur einen Überblick über die besuchten Internetseiten, sondern auch den Zugriff auf das Profil des Sozialen Netzwerkes oder gar im Klartext übertragene Passwörter. Anhand der Hersteller-ID kann der Angreifer sein Opfer sogar direkt identifizieren, wenn im Café nur ein Gast mit einem Gerät dieser bestimmten Marke das WLAN nutzt.

Abhilfe verschafft die Nutzung des VPN der Universität zu Köln. Da-



Foto: istockphoto.com/Yunus_Arakon

bei wird ein verschlüsselter Tunnel zum Server in Köln aufgebaut, über

den dann der gesamte Netzverkehr geleitet wird. Somit sind im WLAN nur noch die sicher verschlüsselten Daten zu sehen und der Angreifer hat keine Möglichkeit mehr in Ihren Netzverkehr zu schauen.

Nutzen Sie unser VPN also nicht nur, wenn Sie Dienste der Universität aufrufen wollen, sondern sichern Sie sich vor Datenspionen in fremden Netzwerkumgebungen.

■ Daniel Böhm
<http://ukoeln.de/CI8EU>

Spam und Spamfilter

Als E-Mail-Spam bezeichnet man unerwünscht zugesandte E-Mails mit meist kommerziellem Inhalt. Es handelt sich häufig um Massensendungen. Schätzungsweise 80–95 Prozent aller heutzutage versendeten E-Mails fallen unter die Kategorie Spam. Ohne Gegenmaßnahmen wird das Medium E-Mail dadurch fast unbenutzbar.

Die Versender solcher E-Mails sind normalerweise nicht ermittelbar. So bleiben nur rein technische Maßnahmen um zumindest die Zustellung des Spams zu verhindern,

Fall sollte man auf solche E-Mails antworten oder einem in der E-Mail angegebenen Link folgen.



Wem die Leistung des RRZK-Spamfilters noch nicht ausreicht, kann natürlich auch selbst weitergehende Maßnahmen ergreifen. Das Einrichten von einfachen Filterregeln („alle Mails mit dem Betreff Viagra löschen“ oder ähnliches) im E-Mail-Portal oder im eigenen E-Mail-Programm ist meist Zeitverschwendung. Spammer variieren ihre unerwünschten Nachrichten ständig, um gerade solche simplen statischen Filter zu umgehen.

Interessanter sind sogenannte bayesschen Filter, wie sie zum Beispiel das E-Mail-Programm Thunderbird (Junk-Filter) anbietet. Diese „lernen“ aus der Entscheidung des Benutzers. Nach der Aktivierung versuchen diese Filter alle E-Mails des Benutzers als „Spam“ beziehungsweise „Nicht-Spam“ zu klassifizieren.

Diese Einordnung ist zunächst einmal nicht sehr effizient. Durch die Korrekturen des Benutzers verbessert sich die Erkennungsrate aber ständig. Nach einiger Zeit sind die Filter auf das individuelle Mailprofil des Benutzers trainiert und erkennen dann recht zuverlässig unerwünschte E-Mails.

■ Susan Barnes
<http://ukoeln.de/DQB5X>



Foto: istockphoto.com/Darko Novakovic

beziehungsweise den Benutzern die Erkennung durch eine entsprechende Markierung zu erleichtern. Zwischen den Versendern (Spammer) und den Anbietern von Filter-Lösungen (Anti-Spam Software) besteht heutzutage eine Art „Wettrüsten“. Spammer versuchen wirksame Filter durch neue Tricks zu umgehen und Hersteller passen ihre Software diesen neuen Methoden wiederum an.

Auch wer die RRZK-Spamfilter in seinem E-Mail-Postfach aktiviert hat, wird gelegentlich trotzdem noch Spam erhalten. Diesen löscht man am besten sofort. Auf keinen

Aktualität bedeutet Sicherheit

Diese Formel verkürzt die Problematik zugegebenermaßen sehr, dennoch kann man sich daran orientieren. Computer, Smartphones, ja selbst Kühlschränke sind inzwischen an das Internet angeschlossen und dort lauern Gefahren. Viren und Würmer machen heute die infizierten Computer unbemerkt zu ferngesteuerten Marionetten, ohne dass der Benutzer es weiß. Diese Schädlinge gehen dabei extrem intelligent vor: Sie können Updates nachladen, um die neuesten Angriffsstrategien zu erfahren. So wird jeder infizierte Computer zu einer ständig besser werdenden Waffe, weitere Computer anzugreifen.

Es bleibt die Frage, wie man sich dagegen schützen kann, und darauf gibt es eigentlich nur eine Antwort: Aktualität beziehungsweise Updates!

Die Angreifer nutzen Program-

mierfehler in der verwendeten Software aus, um sich des Computers zu bemächtigen. Verantwortungsvolle Softwarehersteller geben daher sofort nach Bekanntwerden einer solchen Sicherheitslücke Updates



Foto: istockphoto.com/Giovanni_Meroni

heraus. Da man davon ausgehen kann, dass jede Software derartige Fehler enthält, gilt die Faustformel: Je älter, desto mehr bekannte

Sicherheitslücken, je mehr offene Sicherheitslücken man hat, desto höher ist die Wahrscheinlichkeit, einen Schädling ins System zu bekommen. Und je mehr Menschen unbekümmert und ungeschützt im Internet sind, desto größer die Gefahr für alle anderen „Mit-Surfer“.

Ein Betriebssystem ist nur sicher, wenn es regelmäßig aktuell gehalten wird. Das auf dem Computer beim Kauf vorinstallierte Anti-Viren-Programm, dessen Update-Abonnement abgelaufen ist, bietet kaum zusätzliche Sicherheit. Halten Sie daher all Ihre Softwareprogramme stets aktuell, indem Sie die Updates installieren. Viele Programme verfügen über automatische Updatefunktionen, diese sollten Sie aktivieren. Sie ersparen sich dann, immer selbst drandenken zu müssen.

■ Thomas Oliver Moll

Virenschutz

Der einfache Besuch einer Webseite kann heutzutage schon ausreichen um den eigenen Computer mit Schädlingsprogrammen (Viren, Trojaner, Scareware und so weiter) zu infizieren. Sicherheitslücken in Browsern und browsernaher Software (zum Beispiel PDF-Reader, Flash-Player, Java) machen solche Angriffe („Drive-by-Downloads“) möglich. Regelmäßige Updates bei diesen Programmen sind daher besonders wichtig (siehe weitere Artikel „Aktualität bedeutet Sicherheit“ in dieser Ausgabe). Eine zusätzliche Absicherung bieten Programme, die traditionell noch Anti-Viren-Software genannt werden, obwohl sie natürlich Schutz vor digitalen Plagegeistern aller Art bieten sollen.

Gefahren lauern zudem nicht nur im Web, auch infizierte Dateien auf Netzlaufwerken, USB-Sticks oder E-Mail-Anhänge sind eine ständige Gefahrenquelle. Eine Mammut-

aufgabe also, die diese Schutzprogramme zu bewältigen haben. Die Aktualität ist dabei besonders wichtig – nur ein auf den neuesten Stand gebrachter Virens Scanner bietet einen tatsächlichen Schutz.

Gelangen digitale Schädlinge trotzdem auf den Computer, so liegt deren Augenmerk meist darauf, den Benutzer auszuspionieren. Kreditkarteninformationen, Zugangsdaten zu Onlinebanking oder anderen Websites – es gibt kaum etwas, das die hinter solchen Angriffen stehenden kriminellen Banden nicht zu Geld machen würden. Beliebte ist derzeit auch eine Masche, bei der sich der Schädling als Polizei ausgibt und den Benutzer zur Zahlung einer „Geldbuße“ auffordert – an die Kriminellen, versteht sich.

Die beste Methode der Computer-Säuberung ist in einem solchen Fall die Neuinstallation. Eine geeignete Backup-Strategie voraus-

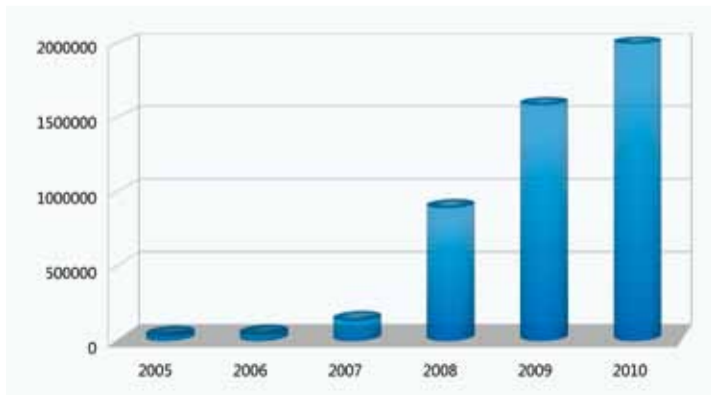
gesetzt (siehe weiterer Artikel in dieser Ausgabe „Datensicherung leicht gemacht“) erlaubt dies schon nach kurzer Zeit wieder sicher am Computer arbeiten zu können. IT-Profis finden im RRZK-Blog zudem Hinweise auf Rettungsmaßnahmen in Situationen, in denen keine Neuinstallation durchgeführt werden kann. Auch der Beratungsdienst des RRZK kann in solchen Fällen bei der Schädlingsbekämpfung behilflich sein.

■ Jens Wahnes

Sophos Anti-Virus
<http://ukoeln.de/XNKIA>

Beratungsdienst des RRZK
<http://ukoeln.de/ULHWP>

RRZK-Blog
<http://ukoeln.de/HLN8L>



Anzahl neuer Schädlingsvarianten pro Jahr



Datensicherung leicht gemacht

Sechs Wochen Arbeit an der Publikation und drei Tage vor Abgabeschluss verweigert Ihre Festplatte den Betrieb? Für Sie kein Problem, denn Sie haben ja eine aktuelle Datensicherung parat und können schnell die letzte Version von gestern Abend wieder herstellen. Wenn die regelmäßigen Backups nur nicht so lästig wären.

Was halten Sie davon, wenn wir das ganz automatisch für Sie übernehmen? Der IBM Tivoli Storage Manager (TSM) ist ein universitätsweiter Backup- und Archivierungsdienst des RRZK. TSM kann mit allen gängigen Betriebssystemen (Windows, Solaris, Linux, MacOS und so weiter) verwendet werden. Mit der TSM-Software können Daten sowohl gesichert (Backup) als auch archiviert (Archive) werden. Die Datensicherung kann dabei vollautomatisiert erfolgen.

Bei einem Backup werden Sicherheitskopien von Dateien oder Verzeichnissen auf dem TSM-Server gespeichert. Diese können bei einem Datenverlust auf dem Arbeitsplatzcomputer vom TSM-Server zurückgeladen werden (Restore). Bei jedem Backup wird die vorherige Sicherungskopie einer Datei durch eine aktuelle Version ersetzt. Verzeichnisse werden nach neuen, geänderten oder gelöschten Dateien durchsucht und dementsprechend auf dem Server aktualisiert. Bereits auf dem Server vorhandene Dateien werden dabei nicht sofort überschrieben, sondern verbleiben noch 30 weitere Tage in einem inaktiven Bereich. Dieses regelmäßige Sichern ist für Dateien geeignet, an denen im Augenblick gearbeitet wird, wie zum Beispiel Diplom- oder Doktorarbeiten. Mit der Archivierungsfunktion

von TSM können Dateien auf dem Server gespeichert werden. Im Unterschied zum Backup bleiben archivierte Dateien auf dem Server bestehen, unabhängig davon, ob sie auf dem Arbeitsplatzcomputer weiter existieren oder nicht. Benötigt man eine archivierte Datei später wieder, wird sie vom Server abgerufen (Retrieve). Archivdaten können manuell verwaltet und gelöscht werden. Die Archivierungsfunktion ist für Dateien geeignet, die nicht mehr bearbeitet, aber für längere Zeit aufgehoben werden müssen, zum Beispiel bereits ausgewertete Daten im Rahmen einer Diplomarbeit.



■ Marc Seifert
<http://ukoeln.de/QHCDJ>

Passwörter: Der tägliche Spagat – Sicher oder leicht zu merken?

Zu den beliebtesten Passwörtern in deutschen Büros zählen „qwertz“, „123456“ und der Name der Partnerin oder des Partners. Für Passwortdiebe ein gefundenes Fressen und innerhalb kürzester Zeit zu knacken.

Tagtäglich geben wir dutzende Male in ein Loginformular unseren Benutzernamen und ein Passwort ein. Bei vielen Anwendungen wäre es jedoch fatal, wenn unser Account geknackt würde und über unser Benutzerkonto zum Beispiel Bestellungen getätigt werden. Ein Passwort zu knacken dauert je nach dessen Komplexität nur wenige Minuten. Die Möglichkeiten, die der Hacker damit erhält, sollten nicht unterschätzt werden.

Es ist vor allem die Menge an Passwörtern, die wir benötigen, die es so schwierig macht sich sichere Passwörter auszudenken, zu verwenden und sie sich auch noch zu merken. Denn EIN „richtig gutes“ Passwort genügt nicht. Bei jeder Anwendung sollte man ein anderes Passwort verwenden und jedes davon sollte

- mindestens aus acht Zeichen bestehen.
- mindestens vier verschiedene Arten von Schriftzeichen enthalten, darunter Großbuchstaben, Kleinbuchstaben und Sonderzeichen.
- kein Name, kein umgangssprachliches Wort, oder irgendein Wort, das auch im Wörterbuch steht, sein.
- weder einen Teil des eigenen Namens, noch die eigene E-Mail-Adresse enthalten.
- regelmäßig geändert werden.
- Und fast am wichtigsten: das Passwort darf nicht aufgeschrieben oder weitergegeben werden.

Nur wie soll das gehen? Hilfreich sind Merksätze in die Teile der jeweiligen Website oder Anwendungen, in die man sich einloggen möchte, eingebaut werden können. Zum Beispiel wird aus dem Merksatz „Es gibt xx Zeichen und die Anfangs- und Endbuchstaben XX“ für die Website rrzk.uni-koeln.de das Passwort „Eg17Z&dA-Ern“.

Je mehr Zeichen ein Passwort hat, umso sicherer wird es, denn umso länger dauert es, es zu knacken.

Aber selbst, wenn all das berücksichtigt wurde, ist ein Pass-



Foto: istockphoto.com/pagadesign

wort nicht mehr sicher, wenn man Opfer von Phishing wird oder im ungeschützten WLAN surft (siehe weitere Artikel in dieser Ausgabe „Phänomen ‚Phishing‘“ und „Datenspiele im öffentlichen Netz“).

■ Ingeborg Wöhr

Computerkurse

IT-Kurse an der Universität zu Köln

Das Regionale Rechenzentrum und die Wiso-IT Services der Universität zu Köln führen regelmäßig in der vorlesungsfreien Zeit Kurse zu verschiedenen Themen rund um IT und Computer durch. Dazu gehören einführende Veranstaltungen zur PC-Benutzung unter Windows ebenso wie Fortbildungen im Bereich PC-Sicherheit, Linux oder Anwendungsentwicklung. Darüber hinaus werden regelmäßig auch Themen wie Grafik und Multimedia, Statistik und eLearning behandelt. Einige Veranstaltungen zum Beispiel zu Office-Anwendungen können im Rahmen des Studiums Integrale angerechnet werden.



Ein ausführliches Verzeichnis der Kurse des RRZK finden Sie in Klips oder unter <http://ukoeln.de/NNEDU>

Ein ausführliches Verzeichnis der Kurse der Wiso-IT Services finden Sie unter <http://ukoeln.de/2W6BN>

Phänomen „Phishing“

Phishing, also das Ausspähen geheimer oder privater Daten durch präparierte E-Mails und Webseiten, ist ein Phänomen des sogenannten Social Engineerings. Im Gegensatz zu altbekannten Methoden wie Computereintritt, Diebstahl oder Erpressung versuchen Phisher die Unbedarftheit ihrer Opfer auszunutzen, sodass diese freiwillig ihre Daten preisgeben. Daher muss ein guter Phisher auch gar nicht so außergewöhnliche und viele Befähigungen besitzen. Klar, ein ordentliches Maß an krimineller Energie kann nicht schaden, aber darüber hinaus muss er vor allem gar kein „großer Hacker“ sein, wie viele vermuten.

Woran erkennt man nun einen Phishing-Versuch? Eine solche E-Mail weist in aller Regel ein paar unverkennbare Eigenschaften auf:

- sie wurde Ihnen unverlangt zugesandt
- sie verwendet anonyme Anreden („Sehr geehrter Herr, sehr geehrte Dame“)
- sie ist in schlechtem Deutsch oder gleich in Englisch verfasst
- sie fordert Sie auf, auf einen eingebetteten Link zu klicken
- sie bittet Sie um Angabe personenbezogener Daten, nach denen seriöse Unternehmen niemals fragen würden, schon gar nicht unverschlüsselt und per E-Mail (Passwörter, PIN, Kreditkartennummern et cetera)

Der Absender ist hingegen überhaupt kein Hinweis auf die Seriosität einer E-Mail, da dieser sehr leicht gefälscht werden kann. Da-

her hat es auch keinen Sinn, sich beim (angeblichen) Absender zu beschweren, da dieser in der Regel gar nichts von dieser Mail weiß.

Was soll man nun mit Phishing-



Foto: istockphoto.com/Paul_Gregg

Mails tun? Die Antwort ist einfach: Löschen! Keinesfalls sollte man auf die E-Mail antworten, auch eine Weiterleitung zum Beispiel an das RRZK ist sinnlos, da wir gegen die Urheber leider nichts unternehmen können. Unsere Benutzer haben wir vielfach mittels diverser Informationskanäle auf die Gefahr hingewiesen, hier müssen wir nun auf den gesunden Menschenverstand vertrauen.

Um das Aufkommen von Phishing in Ihrem Posteingang zu minimieren, empfehlen wir den Einsatz des Spamfilters, den Sie im Mailportal konfigurieren können. Zwar erwirkt dieser auch nicht alles, aber die Menge sollte doch deutlich reduziert werden.

■ Patrick Holz
<http://ukoeln.de/V46XP>



Impressum

Herausgeber:
Der Rektor der Universität zu Köln

Redaktion:
Regionales Rechenzentrum
Prof. Dr. Ulrich Lang (Leitung)
Dr. Marc Seifert
Ingeborg Wöhr

Anschrift:
Robert-Koch-Straße 10
50931 Köln
Telefon 0221 478-7019
Telefax 0221 478-5568
E-Mail it-beilage@uni-koeln.de

Auflage: 13.000 Exemplare

Gestaltungskonzept:
Dipl. Des. Rona Duwe
zefo | Zentrum für Forschungskommunikation | www.zefo.de

Satz und Layout dieser Ausgabe:
mehrwert intermediale kommunikation GmbH | www.mehrwert.de

Druck:
Köllen Druck + Verlag GmbH
Ernst-Robert-Curtius-Straße 14
53117 Bonn-Buschdorf