Dipl.-Ing. Dr. Kurt P. Judmann
Präsident des Landesverbandes für Wien, Niederösterreich und Burgenland

Internetnutzung – über Risken und deren Vermeidung*

Das Internet ist eine etablierte und weltweit genutzte Informationsquelle geworden. Es bildet darüber hinaus die Basis für vielfältige Kommunikationsmöglichkeiten im privaten Bereich, zwischen Unternehmen und auch mit Behörden.

Um die Möglichkeiten des Internets nutzen zu können, ist ein Computer erforderlich, der zumindest zum Zeitpunkt der Verwendung „Teil des öffentlichen Internets" ist. Das bedeutet, dass der Computer mit den standardisierten Methoden, mit denen Kommunikationen im Internet aufgebaut und abgewickelt werden, ansprechbar sein muss. Wie auch bei einer herkömmlichen Kommunikation wird dazu eine Adresse verwendet. Damit werden die teilnehmenden Computer im Internet eindeutig identifiziert und angesprochen. Werden keine besonderen Vorkehrungen getroffen, kann jeder Computer im Internet jeden anderen ansprechen. Aus der großen Anzahl von Computern, für die dies möglich ist, und der internationalen Verteilung sowie der daraus resultierenden Anonymität, hinter der sich Angreifer verbergen können, resultieren spezifische Risken bei der Nutzung des Internets.

1. Grundlagen

Ein besonderes Prinzip im Internet besteht in der Verwendung standardisierter Dienste. Dabei handelt es sich um Programme, die auf den teilnehmenden Computern ablaufen, die dazu dienen, auf bestimmte empfangene Daten in einer dem Dienst entsprechenden, vordefinierten Art automatisch zu reagieren.

Eine weitgehend bekannte Anwendung dafür stellt das „World Wide Web" dar. Dabei werden im Internet Computer verwendet, die als Server bezeichnet werden. Ihre primäre Aufgabe ist es, automatisiert auf Anfragen zu antworten. Spricht man einen derartigen Server in der dafür vorgesehenen Art und Weise, beispielsweise mit einem Webbrowser an, werden automatisch jene Inhalte zurückgeliefert, die auf der Website dargestellt werden.

Solche und ähnliche Dienste können sich allerdings auch auf Laptops und Arbeitsplatzrechnern in Ausführung befinden, sodass man in ähnlicher Art und Weise auch einen einfachen Laptop, der gerade mit dem Internet verbunden ist, ansprechen kann. Dieser wird, wenn dabei ein zutreffender Dienst angewählt wurde, automatisch antworten. In diesem Zusammenhang spricht man von „Ports", das sind Zugänge zu den einzelnen Computern, die als Kennung für bestimmte Dienste, über die Adressen erreichbar sind, dienen.

Durch die große Anzahl der auf diese Art und Weise miteinander weltweit verbundenen Computer und der für den Benutzer undurchschaubaren Art und Weise, wie Kommunikation zwischen den Computern initiiert wird und wie sie abläuft, verliert man die Kontrolle darüber, welche Informationen aus dem eigenen System automatisiert weitergegeben werden und auch welche Programme durch Eingriffe von außen auf einem lokalen Computer, allenfalls auch unbemerkt, gestartet werden. Es ergeben sich Bedrohungen, die einer Berücksichtigung und auch entsprechender Maßnahmen bedürfen.

2. Angriffe aus dem Internet

Neben Angriffen, die aus dem Internet auf die damit verbundenen Computer wirken, bestehen auch noch weitere Gefahren, die im Zusammenhang mit der Verbindung zum Internet stehen. Während die direkten Angriffe aus dem Internet mit einer aus dem Internet initiierten Kommunikation und dem Versuch zusammenhängen, Reaktionen, die vom Benutzer des Computers so nicht vorgesehen sind, hervorzurufen, gibt es auch indirekte Angriffe, die von dem attackierten Computer selbst ausgehen. Die bekannteste Quelle dafür sind sogenannte „Schadprogramme". Dazu

* Der vorliegende Artikel stellt eine Zusammenfassung des Vortrages dar, den der Autor am 12. 1. 2010 beim 7. Fachseminar für Sachverständige und Juristen „Spezielles aus Recht und Praxis im Sachverständigenwesen" in Bad Hofgastein gehalten hat.

gehören auch Computerviren, die auf unterschiedliche Art und Weise auf einen Computer gelangen können. Solche Programme verursachen häufig nicht unmittelbar ersichtliche Effekte, die dem Benutzer sofort auffallen. Sie können das Internet auch dazu verwenden, um die Kommunikation zu anderen Computern aufzubauen und die Ressourcen und Daten des befallenen Computers über das Internet zugängig zu machen.

Eine besonders aktuelle Version solcher Schadprogramme ist jene, die vom Benutzer unbemerkt die Abfolge von Tastenbetätigungen registrieren und diese periodisch über das Internet an andere Computer übermittelt. Aus den auf diese Art und Weise weltweit automatisiert gesammelten Daten lassen sich leicht jene Abfolgen herausfinden, die man aufgrund ihrer Struktur als Kreditkartennummern identifizieren kann.

Eine völlig andere Gefahr entsteht durch die praktische Abhängigkeit der Benutzer von IT-Systemen im Privat- und vor allem im Geschäftsleben. Ein Funktionsverlust, der durchaus auch durch einen Defekt eintreten kann, kann dabei, wenn nicht speziell Vorsorge dafür getroffen ist, zu wesentlichen Beeinträchtigungen für erforderliche Aktivitäten führen.

3. Bedrohungen und Risken

Im Weiteren sind wichtige Bedrohungen ihrer Art nach dargestellt und Beispiele für Auswirkungen dieser Bedrohungen und grundsätzliche Gegenmaßnahmen aufgezeigt. Diese Aufstellung ist keineswegs vollständig, sie soll lediglich dazu dienen, dem Leser einen Einblick über die Vielfältigkeit von Bedrohungen, die häufig gar nicht bewusst werden, zu geben.

3.1. Direkte Angriffe

Dabei handelt es sich um die schon vorstehend erwähnte Möglichkeit, jeden Computer im Internet ansprechen zu können. Sie kann dazu missbraucht werden, zu versuchen, Dienste auf Computern zu aktivieren, mit denen man unauthorisierten Zugriff auf Daten und Ressourcen erhält.

Jeder Computer im Internet hat eine eindeutige Adresse, die sogenannte IP-Adresse. Für jede IP-Adresse können unterschiedliche sogenannte „Ports“ angesprochen werden, die entsprechend der Standardisierung zu unterschiedlichen Reaktionen, beispielsweise auch zu Programmaufrufen im Computer führen können. Ein bloß temporär mit dem Internet verbundener Computer erhält eine temporäre IP-Adresse, die nicht allgemein bekannt ist. Angreifer sind daher darauf angewiesen, entweder Computer anzusprechen, die immer dieselbe IP-Adresse aufweisen (statische IP-Adressen), wobei diese beispielsweise deswegen bekannt sind, weil es sich um einen Server handelt. Sie können aber auch einfach durch „Probieren“ herausfinden, an welcher IP-Adresse ein Computer reagiert und somit angeschlossen ist. Bei der großen Anzahl von Teilnehmern im Internet und wegen des Umstandes, dass man derartige Versuche, Computer einfach durch zufälliges Ansprechen einer Adresse zu lokalisieren, nicht offensichtlich bemerkt, haben Angreifer ein großes Potenzial und viel Zeit, um automatisiert zum Erfolg zu gelangen. Wird auf diese Art und Weise ein Computer identifiziert, kann der Angreifer darangehen, zu versuchen, über welchen der möglichen Ports – das sind einfach Nummern, denen vordefinierte Dienste und Reaktionen zugeordnet sind – der Computer reagiert. Dazu gehört der bekannte Begriff „Port Scan“. Handelt es sich um einen Computer, bei dem eine ungeschützte und uneingeschränkte Systeminstallation vorliegt, können über diese Ports Dienste aktiviert werden, mit denen es je nach Einstellung gelingen kann, die Kontrolle über den Computer zu ergreifen. Programme können auf den Computer geladen und zur Ausführung gebracht und zur Ausspähung verwendet werden.

Wichtige Gegenmaßnahmen in Hinblick auf solche Attacken bestehen darin, die IP-Adresse eines Computers von vorneherein von außen nicht „sichtbar“ zu machen. Dazu werden spezielle Geräte oder Programme (Firewalls) verwendet. Sie stellen das Bindeglied zwischen einem Computer bzw auch einem Computernetzwerk und dem Internet dar. Ein derartiges Gerät bzw ein Computer mit einem solchen Programm hat im Internet ebenfalls eine IP-Adresse. Die IP-Adresse des tatsächlich verwendeten Computers und damit auch der Zugriff darauf wird verborgen. Auf diese Art und Weise können Computer im Internet durch zufälliges Ansprechen von IP-Adressen nicht aufgefunden werden. Diese Geräte erlauben es auch, das Ansprechen einzelner Dienste über Ports zu kontrollieren. Das muss dazu genützt werden, um nur jene Ports zu aktivieren, die man für die bestimmte Computeranwendung auch tatsächlich benötigt. Auch auf den Computern selbst muss man in diesem Zusammenhang Sorge tragen, dass beim Einschalten lediglich jene Dienste automatisch gestartet werden, die tatsächlich erforderlich sind. Es dürfen keine Programme ausgeführt werden, die automatisiert auf Ports reagieren, die man nicht benötigt.

3.2. Indirekte Angriffe

Bei indirekten Angriffen handelt es sich um Auswirkungen von Programmen, die auf einem Computer ausgeführt werden. Sie bewirken von den befallenen Computern aus, dass dieser aktiv auf das Internet und damit auf andere Teilnehmer zugreift. Die Grundlage eines solchen Angriffes besteht darin, dass ein Programm, das für schädliche Wirkungen verwendet werden kann, auf irgendeine Art und Weise auf den Computer gelangt ist und dort ausgeführt wird. Wie bereits vorstehend dargestellt, kann es sich dabei um Computerviren handeln, mit denen Daten des Computers ausgespäht werden.

Eine verbreitete Missbrauchsmöglichkeit besteht auch darin, dass Programme, die automatisch Dateien über das Internet austauschen, von einem Benutzer geladen und im Weiteren auch über längere Zeit unbemerkt automatisch ausgeführt werden. Dabei handelt es sich häufig um Programme für Tauschbörsen, die dazu dienen, von unterschiedlichen, zum Teil ebenfalls „anonymen" Computern im Internet Dateien – zB Filme oder Audiodateien – zu laden. Solche Tauschbörsen funktionieren häufig so, dass jeder Computer, der mit diesen Mitteln aus dem Internet Dateien beziehen will, jene Dateien, die er gerade auf dem Computer hat, auch für andere Benutzer, die dieselbe Datei suchen, zur Verfügung stellt. Dies geschieht automatisch. Hat man die Datei auf dem Computer und hat man das entsprechende Programm in Ausführung, wird der Computer von anderen „Suchenden" gefunden und die Datei wird vom eigenen Computer an den abfragenden Computer übertragen.

Wenn dies unbemerkt geschieht, ergeben sich häufig weitreichende Konsequenzen. Die einfachste davon ist dabei noch der Umstand, dass solche Vorgänge einen hohen Datenverkehr erzeugen können, der beispielsweise bei mobilen Internetanschlüssen unerwartete Gebühren hervorrufen kann. Es kann aber nicht ausgeschlossen werden, dass mit solchen Diensten illegale Inhalte auf den eigenen Computer und von dort wiederum an andere Benutzer gelangen, ohne dass man dies bemerkt. Solche Aktivitäten können dann auch Gegenstand behördlicher Untersuchung und der Strafverfolgung werden.

Eine Maßnahme gegen dieses Risiko besteht ebenfalls in der Verwendung von Firewalls, mit denen solche Dienste automatisch blockiert werden. Weiters ist auch die Verwendung aktueller Antivirenprogramme, mit denen die Wirkung von Schadprogrammen auf den Computern hintangehalten werden soll, eine grundlegende Sicherheitsmaßnahme. Ein wichtiges Grundprinzip dabei ist vor allem auch das Bewusstsein, dass die Verwendung solcher Programme wie beispielsweise jener von Tauschbörsen genau zu überdenken ist und man wissen muss, inwieweit die Verwendung eines solchen Programmes eventuell unbeobachtet und unbemerkt weiterläuft und welche Konsequenzen dies haben kann.

3.3. Sicherheitsverlust und Verluste der Privacy

Die Verbindung eines Computers, auf dem Daten gespeichert sind, die zum Teil einer persönlichen oder geschäftlichen Geheimhaltung unterliegen, mit dem Internet stellt ein Risiko dar. Mit den vorstehend dargestellten technischen Methoden können solche Daten ausgespäht werden. Allerdings führt die Verwendung eines Computers mit solchen Daten auch ohne spezielle Attacken zu einem Sicherheitsrisiko, für das ein Bewusstsein entwickelt werden muss.

Bei der Übermittlung von Daten, Geschäfts- oder Bankinformationen, bei der Anmeldung an E-Commerce-Seiten und der Abwicklung von Geschäften, wie dies nicht nur zweckmäßig, sondern auch sehr bequem und effizient ist, werden Daten übertragen, die für die Allgemeinheit nicht bestimmt sind. Dabei kann es sich zB um persönliche Daten handeln, Informationen über Reisen und natürlich auch um Bankdaten. Solche Daten müssen geheim gehalten werden, das bedeutet, sie müssen sowohl auf dem Computer als auch auf dem Übertragungsweg – zB durch Verschlüsselung – geschützt werden. Weiters muss sichergestellt werden, dass bei der Kontaktaufnahme mit anderen Computern und der Übermittlung solcher Daten die Authentizität gewahrt bleibt und sichergestellt ist, dass man nur mit jenem Computer bzw jenem Geschäftspartner Daten austauscht, mit dem man dies tatsächlich möchte und vermeint, es zu tun.

Die Schutzmaßnahmen zur vorstehenden Thematik betreffen den Bereich der Kryptografie. Dem Risiko kann nur vorgebeugt werden, indem ausschließlich Programme und Einstellungen verwendet werden, für die plausibel gemacht ist, dass entsprechende Sicherheitsstandards eingehalten sind. Das bedeutet, dass man bei der Verwendung von Computerprogrammen, beim Ansprechen von E-Commerce-Seiten jedenfalls darauf achten muss, es mit etablierten und vertrauenswürdigen Partnern zu tun zu haben.

Ein sehr aktuelles Thema in diesem Zusammenhang stellt die ungewollte Preisgabe von persönlichen Informationen im Zuge der Nutzung von allgemeinen Webdiensten dar.

Die Anbieter von Informationsseiten – dabei kann man an Suchmaschinen, an Medien, Geschäftsseiten mit Angeboten etc denken – sammeln mit den im Internet zur Verfügung stehenden Methoden Informationen über jene Computer und auch Benutzer, die diese Dienste nützen. Damit lassen sich automatisiert Aufzeichnungen über das Benutzerverhalten gewinnen. Beispielsweise lässt sich einfach feststellen wie lange bestimmte Seiten in Informationsangeboten aufgerufen werden, von wo eine bestimmte Seite aufgerufen wird und zu welcher anderen Seite man verzweigt. Vielfältige, den Techniken des Web 2.0 und den aktuellen Kommunikationsmethoden zuzuordnende Dienste erfordern Anmeldedaten und persönliche Informationen, um die Vorteile der Dienste nutzen zu können. Über solche Anmeldedaten lassen sich Benutzerprofile von unterschiedlichen Stellen automatisch zusammenführen und auf diese Art und Weise eine Unzahl von Informationen über das individuelle Verhalten eines Internetteilnehmers sammeln. Eine besondere Bedrohung stellen jene Kommunikationssysteme dar, die bei der Anmeldung darauf abzielen, lokal am Computer gespeicherte Daten, beispielsweise Outlook-Adressbücher, automatisiert anzusprechen und diese Daten dem Benutzerprofil zuzuordnen. Dies mag für Community-Systeme wie „Facebook“ sehr praktisch sein. Nach der Anmeldung – drückt man nur an einer Verzweigung eine falsche Taste – erfahren alle Personen, die man im Adressbuch gespeichert hat, dass man dem Dienst beigetreten ist. Natürlich werden diese Personen dem eigenen Profil zugeordnet und weiterverarbeitet.

Auch dabei muss der Benutzer die Gefahren kennen und kritisch hinterfragen, ob der Vorteil der jeweiligen Dienste die in Kauf zu nehmenden Privacy-Verluste und Nachteile aufwiegt. Jedenfalls ist es empfehlenswert, aktuelle und korrekte Benutzerdaten in solche Systeme nicht einzugeben, sondern Synonyme zu verwenden. Auch dabei muss man große Vorsicht aufwenden, denn durch die automatisierten Auswertungen wird, sollte nur an einer Stelle ein Zusammenhang zwischen einem echten Namen und dem Synonym herstellbar sein, letztlich sämtliches Benutzerverhalten zusammengeführt.

4. Auswirkungen

Die vorstehende Aufzählung enthält lediglich einige besonders naheliegende Angriffsmöglichkeiten sowie Gefahren und Auswirkungen, denen man als Internetbenutzer ausgesetzt ist.

Die Auswirkungen von Attacken über das Internet können für den einzelnen Benutzer gravierend und vor allem überraschend sein. Dies ergibt sich aus jenen Möglichkeiten für Attacken, die vom Benutzer weitgehend unbemerkt bleiben. Vor allem die Möglichkeit, dass private Computer unbemerkt nach entsprechenden Attacken dazu verwendet werden können, um über diese Computer wiederum Attacken gegen andere Computer ablaufen zu lassen, bzw dass diese Computer dazu benützt werden können, illegale Daten und Informationen – zB Kinderpornografie – zu verteilen, kann zu einem wesentlichen Problem werden. Dabei stellt sich immer die Frage, ob man dem Benutzer des Computers vorwerfen kann, dass er die übliche Sorgfalt bei der Verwendung eines Computers und des Internets nicht beachtet. In Hinblick auf die in den Medien vielfach publizierten Angriffe, Viren und kriminellen Vorgänge, die mit Hilfe des Internets ausgeführt werden, ist das erforderliche Maß an Sorgfalt nun bereits schon hoch zu bewerten. Dazu ist auch festzustellen, dass im Allgemeinen jeder Computerbenützer wissen muss, dass man Antivirenprogramme benötigt, um zumindest einen grundlegenden Schutz zu erhalten, und dass man den eigenen Computer zumindest auch mit den in den Betriebssystemen vorgesehenen Methoden – zB bei Windows mit der dort vorgesehenen Firewall – gegen das Internet schützen muss. Jeder, der ein Programm für eine Tauschbörse verwendet, muss sich klar darüber sein, dass der Bezug von Daten mit großer Wahrscheinlichkeit auch zur Folge hat, dass über den eigenen Computer auch Daten verteilt werden. Er muss daher dafür Sorge tragen, dass das nicht unbemerkt und vor allem nicht mit unbekannten Inhalten erfolgt.

Die Liste der Konsequenzen aus solchen Missbräuchen, die zu Überraschungen und auch zu einer strafrechtlichen Problematik führen können, ist groß. Zusammenfassend kann in Anbetracht dieser Problematik und der dynamischen Entwicklung bei neuen Attacken und bei zugehörigen Gegenmaßnahmen als wichtigste Empfehlung die Schärfung des Bewusstseins für diese Thematik empfohlen werden. Das Mindestmaß an Sorgfalt setzt dabei einerseits ein kritisches Hinterfragen der verwendeten Programme und Dienste und der Systeminstallation voraus und, falls das entsprechende technische Fachwissen oder die zur Verfügung stehende Zeit für eine Befassung mit diesem Thema nicht ausreichen, das Erfordernis, sich den Rat eines Experten bei der Einrichtung des Computers zu holen.

Korrespondenz:
Dipl.-Ing. Dr. techn. Kurt P. Judmann
Telefon: 01 / 586 64 46
E-Mail: k.judmann@gerichts-sv.org