Institut für Rundfunktechnik

Technischer Bericht

Abschlussbericht Projekt V-Security **Nr. B 198/2007**

**Bericht**
**Nr. B 198 / 2007**

# Abschlussbericht Projekt V-Security


**Inhaltsangabe**

Das Projekt V-Security befasste sich 2005 schwerpunktmäßig mit der Erkennung und Dokumentation von Sicherheitsrisiken in Rundfunknetzen, speziell Zuspiel- und Verteilnetzen, sowie Performanzuntersuchungen im Zusammenhang mit Security Mechanismen (z.B. Reduzierung der verfügbaren Übertragungsgeschwindigkeit durch den Einsatz von Firewalls). Der Fokus der messtechnischen Untersuchungen in 2005 lag hierbei auf dem Videofiletransfer. Die Ergebnisse wurden unter anderem in mehreren Vorträgen (FKTG, EBU) präsentiert. Der Abschlussbericht wird dem IT-Sicherheitsgremium für das ARD-CN zur Verfügung gestellt.


München, Mai 2007


Verfasser:

Herbert Guist
Speicher und Netze im Rundfunk

Mathias Hammer
Speicher und Netze im Rundfunk

Markus Berg
Speicher und Netze im Rundfunk


Verteiler:
AKAS
AKO
ARV
IRT
AG Informatik
ASF
Leiter Fernseh-Betrieb
Leiter Hörfunk-Betrieb
Leiter Sender-Betrieb
PTKO


INSTITUT FÜR RUNDFUNKTECHNIK GmbH

Dr. Klaus Illgner
Direktor und Sprecher der Geschäftsleitung

## Sicherheit ist Chefsache

Sicherheit ist ein Grundbedürfnis des Menschen und damit unserer Gesellschaft. Durch die zunehmende Abhängigkeit von der Technik - ein Leben ohne Informations- und Kommunikationstechnik ist heute kaum noch vorstellbar - nimmt das Sicherheitsbedürfnis weiter stark zu. Viele Unternehmen wären in ihrer Existenz bedroht, würde ihre IT-Technik über einen längeren Zeitraum ausfallen. Bereits kurzzeitige Ausfälle verursachen für viele schon hohe Kosten.

Die Komplexität der IT-Systeme hat in den letzten Jahren stark zugenommen, das hat zur Folge dass selbst IT-Sicherheitsexperten Mühe haben, den Überblick zu behalten. Gleichzeitig ist die Gefahr, Opfer einer Attacke zu werden - egal ob beabsichtigt oder nicht - gestiegen. Dennoch ist die Ansicht weit verbreitet, dass IT-Sicherheitsmaßnahmen aus Sicht der Verantwortlichen mit hohen Investitionen verbunden sind und aus Sicht der Belegschaft meist unbequem sind, da sie höhere Disziplin erfordern und häufig Einschränkungen im Bedienkomfort nach sich ziehen.

Auch das persönliche Sicherheitsbedürfnis mancher Verantwortlichen führt zu Fehleinschätzungen. Oft hört man Ausdrücke wie:

- *"bei uns ist noch nie etwas passiert"* - zumindest hat keiner etwas bemerkt.
- *"unser Netzzugang ist sicher"* - auch kommerzielle Firewalls haben Fehler. Hat der Admin auch wirklich alle Updates eingespielt? Auch Administratoren sind Menschen und können mal etwas übersehen haben.
- *"unsere Mitarbeiter sind vertrauenswürdig"* - aber die Statistik spricht dagegen. Ca. 80 % der Angriffe erfolgen aus dem internen Netz. Dabei handelt es sich selten um vorsätzliche Angriffe, in den meisten Fällen werden die Probleme durch Unachtsamkeit, Übereifer und Neugier verursacht.
- *"bei uns ist nichts zu holen"* - in den meisten Unternehmen gibt es Daten, die, wenn sie in falsche Hände geraten zwar nicht die Existenz des Unternehmens bedrohen, aber zumindest unangenehme Folgen wie Imageverlust zur Folge haben.

Auf die wachsende Gefahr massiver wirtschaftlicher Schäden in Folge von IT-Sicherheitsvorfällen hat auch der Gesetzgeber reagiert und verschiedene Regelungen und Gesetze erlassen, die dafür sorgen, dass Vorstände bzw. Geschäftsführer persönlich für Versäumnisse haften. Somit gilt: Sicherheit ist Chefsache! Für bestimmte Berufsgruppen wie Ärzte und Rechtsanwälte gibt es sogar Sonderregelungen im Strafgesetzbuch, die zu besonders sorgfältigen Umgang mit den Daten ihrer Patienten und Mandanten anregen sollen. Mittlerweile sind Banken dazu gezwungen, bei der Kreditvergabe auch eventuelle IT-Risiken des Kreditnehmers zu prüfen, eine Maßnahme, die sich unmittelbar auf die angebotenen Konditionen auswirkt.

Was sind so die häufigsten Fehler und Versäumnisse? Untersuchungen des BSI (Bundesamt für Sicherheit in der Informationstechnik) haben gezeigt, dass die typischen Mängel weder von der Unternehmensgröße, noch von der Branche abhängig sind, auch wenn größere Unternehmen in puncto Sicherheit meist weniger Defizite aufweisen.

- **Fehlende oder unzureichende Sicherheits-Strategie:** in vielen Unternehmen hat IT-Sicherheit einen geringen Stellenwert. Man scheut die Investitionen und fürchtet sich vor Verschlechterungen in Bedienkomfort und/oder Funktionalität. Hinzu kommt oft noch reine Bequemlichkeit und zu mangelndes Fachwissen über Risiken. Bei der Planung größerer Projekte werden Sicherheitsaspekte häufig erst sehr spät berücksichtigt, wenn nicht gar erst im Nachhinein überhaupt die ersten Sicherheitsfragen auftauchen. Das wiederum erhöht den Aufwand und treibt die Kosten in die Höhe. Besser ist es, Sicherheitsanforderungen bereits in die frühe Planungsphase mit ein zu beziehen, Schwachstellenanalysen durchführen und entsprechende Maßnahmen auszuarbeiten. Diese sind schriftlich festzuhalten und bei der Umsetzung einzuhalten. Auch sollte beachtet werden, dass die meisten IT-Systeme im Produktivbetrieb im Laufe der Zeit durch neue Anforderungen andere Konfigurationen und Parameter benötigen. Um die Sicherheit zu gewährleisten muss in regelmäßigen Abständen überprüft werden, ob die ursprünglichen Anforderungen noch eingehalten werden. Eine vernünftige Sicherheits-Strategie erfordert klare Zuständigkeiten und stellt sicher, dass Sicherheit eine zeitlich unbegrenzte Aufgabe ist. Unbedingt erforderlich ist eine schriftlich fixierte Sicherheitsrichtlinie, die für alle Mitarbeiter verbindlich ist. Diese sollte klar formuliert sein und ihre Einhaltung kontrolliert werden.

- **Schlechte Konfiguration der IT-Systeme:** eine goldene Regel bei der Arbeit eines Administrators lautet: gib deinen Nutzern so viele Rechte wie nötig und so wenige wie möglich. Das gleiche Prinzip sollte allerdings auch für ihn selber gelten. Natürlich ist es bequemer, administrative Aufgaben zu erledigen ohne sich neu anzumelden. Durch die ständig wachsende Komplexität neuer (häufig vernetzter) Anwendungen steigt na-

türlich auch der Arbeitsaufwand für Administratoren und damit das Risiko einer unsicheren Konfiguration. Sicherheit stellt nur eine Aufgabe unter vielen, zum Teil konkurrierenden Aufgaben dar.

• **Unsichere Vernetzung und Internet-Anbindung:** mittlerweile sollte es kaum noch Unternehmen geben, deren Internet-Zugang nicht durch eine Firewall abgesichert ist. Die große Anzahl neuer Applikationen deren sichere Anbindung an das Internet oft spezielle Kenntnisse erfordert, erhöht natürlich auch das Risiko einer Fehlkonfiguration der Firewall. Auch wenn heute systembedingte Sicherheitslöcher nur noch selten vorkommen, sollte die Firewall in regelmäßigen Abständen von externen Sicherheitsspezialisten überprüft werden.

• **Nichtbeachtung von Sicherheitserfordernissen:** häufig werden Sicherheitsrichtlinien missachtet und Sicherheitsfunktionen nicht genutzt. Vertrauliche Daten benötigen besonderen Schutz. Der Zugriff auf sie sollte passwortgeschützt sein und protokolliert werden. In der Vergangenheit ist es häufig vorgekommen, dass Viren und Trojaner über Notebooks in Unternehmen eingeschleppt wurden und über deren Schadfunktionen vertrauliche Daten in falsche Hände geraten sind. Gegen solche Angriffe bieten Firewalls kaum Schutz. Da kann es durchaus Sinn machen, den Inhalt von Dateien und Ordnern mit vertraulichen Daten zu verschlüsseln. Der erfolgreichste Angriff ist auch heute noch das so genannte "social hacking". Dabei werden z.B. ahnungslose Mitarbeiter von angeblichen neuen Mitarbeitern aus der Datenverarbeitung nach ihren Passwörtern gefragt oder dem sprichwörtlichen "Handwerker im Blaumann" ohne irgendwelchen Verdacht die Türen zu Räumen mit vertraulichen Daten geöffnet. Das ist in der Regel kein Angriff eines Script-Kiddies sondern ein hoch bezahlter Industriespionage-Angriff.

• **Schlechte Wartung der Systeme:** der Zeitpunkt zwischen dem Bekanntwerden eines Sicherheitslochs und dem Auftreten von Schädlingen, die diese Schwachstellen ausnützen, liegen immer näher beieinander. So genannte Script-Kiddies basteln Würmer und Trojaner mittels weniger Mausklicks binnen Minuten zusammen. Die Tools dafür sind für jedermann kostenlos im Internet zu haben. Für alle Sicherheitslöcher, die von den großen Virenangriffe der letzten Jahre ausgenutzt wurden, hat es seitens der Hersteller rechtzeitig Sicherheits-Updates gegeben. Hätten alle Administratoren die Updates eingespielt, hätten Würmer wie CodeRed, W32Blaster und Sasser keine Chance gehabt!

• **Sorgloser Umgang mit Passwörtern und Sicherheitsmechanismen:** auch heute noch werden Einbrüche in Systeme bekannt, weil immer noch Passwörter unter der Tastatur, am Bildschirm oder der obersten Schreibtischschublade aufbewahrt werden. Auch werden häufig unsichere Passwörter verwendet (zu kurz oder leicht erratbar). Sicherheitsspezialisten verwenden Tools, um schwache Passwörter aufzuspüren, das sind im Übrigen die gleichen Tools, die von Hackern für ihre Einbrüche eingesetzt werden. Untersuchungen von Fachzeitschriften haben gezeigt, dass drahtlose Netzwerke (WLANs) inzwischen auch in Unternehmen weit verbreitet sind, deren Sicherheitsmechanismen aber oft aus Bequemlichkeit oder Kompatibilitätsgründen nicht auf höchster Stufe konfiguriert (WEP statt WPA) oder gar ausgeschaltet sind.

• **Mangelhafter Schutz vor Einbrechern und Elementarschäden:** unverschlossene IT-Räume, über Nacht gekippte Fenster, Notebooks die in Autos zurückgelassen werden machen es Einbrechern und Dieben leicht, Hardware zu erbeuten. Der Verlust der Hardware ist dabei noch meist das geringere Übel, Daten die nicht ausreichend gesichert wurden sind da meist viel schwieriger wieder zu beschaffen, ganz zu schweigen von dem Fall, dass vertrauliche Daten in falsche Hände geraten. Aber auch die glücklicherweise seltenere Ereignisse wie Feuer- und Wasserschäden können fatale Folgen haben. Gut, wenn dann ein halbwegs aktuelles Backup existiert, welches nicht in dem gleichen Gebäudeteil gelagert wurde, in dem die Datenverarbeitung vernichtet wurde. Brandschutz und Schutz vor Wasserschäden sollten Bestandteil einer guten Sicherheits-Strategie sein.

## Schritt für Schritt zu mehr Sicherheit

Der beste, wenn auch teuerste Weg, ein Sicherheitskonzept zu erstellen, ist eine traditionelle Risikoanalyse. Darin werden die schutzbedürftigen Werte ermittelt und deren Bedrohung untersucht. Dazu gehören nicht nur die IT-Systeme (Hard- und Software) sondern die Daten ebeso wie das Know-how. Als Ergebnis erhält man eine so genannte Bedrohungsmatrix, die einen Überblick über die Wahrscheinlichkeit eines Sicherheitsvorfalls und den zu erwartenden Schaden liefert. Das erlaubt das Ausarbeiten individueller Schutzmaßnahmen für die vorliegende IT-Landschaft.

Wer die Kosten einer Risikoanalyse scheut - in der Regel benötigt man dazu externe Sicherheitsexperten - dem bietet das IT-

Grundschutzhandbuch des BSI eine kostenlose und effektive Alternative. Es erlaubt dem Sicherheitsbeauftragten Schritt für Schritt eine Verbesserung der IT-Sicherheit. Im ersten Schritt werden die vorhandenen IT-Systeme (Hard- und Software, Applikationen) und IT-Räume erfasst. Im zweiten Schritt gilt es zu ermitteln, wie hoch der Aufwand für eine Verbesserung des Schutzes der IT-Landschaft ist. Dann geht es an die Umsetzung der Richtlinien, dabei werden nach und nach alle Komponenten auf Sicherheit geprüft und ggf. optimiert, das Handbuch enthält umfangreiche Listen zu zahlreichen Komponenten (die aktuelle Fassung vom Dezember 2004 ist immerhin 2908 Seiten stark). Es wird sich herausstellen, dass in zahlreichen Fällen gar keine Investitionen nötig sind. Viele Verbesserungen sind durch Optimierung der Parameter zu erzielen oder durch geringe organisatorische Maßnahmen. Je intensiver Mitarbeiter in diese Prozesse eingebunden werden, desto mehr Verständnis werden sie für Veränderungen haben, das Sicherheitsbewusstsein wird gefördert, ein nicht zu unterschätzender Faktor, der signifikant zur Erhöhung der gesamten IT-Sicherheit beiträgt.

Um den Nachweis zu erbringen, dass definierte Sicherheitsstandards eingehalten werden, lassen sich immer mehr Unternehmen und Organisationen zertifizieren. Die bekanntesten sind dabei ISO 17799, BS 7799-2 und ITIL (IT Infrastructure Library). Neuerdings bietet auch das BSI eine Zertifizierung nach dem IT-Grundschutzhandbuch an, seit Januar 2006 sogar nach dem neuesten Standard ISO 27001. Nach Umsetzung aller für eine Zertifizierung erforderlichen Maßnahmen kann die Organisation einen lizensierten Auditor beauftragen, der die IT-Infrastruktur gemäß dem BSI-Prüfschema überprüft. Gegen Vorlage des Auditreports kann beim BSI die Zertifizierung beantragt werden.

## IT im Rundfunk

Noch vor wenigen Jahren waren die Rundfunkanstalten abgeschlossene Inseln doch der Siegeszug des Internet hat auch vor ihren Toren nicht Halt gemacht. Für viele Redaktionen ist die tägliche Arbeit ohne Zugang zum Internet kaum noch denkbar. Hinzu kommt ein Zusammenwachsen der klassischen Rundfunk- mit der IT-Welt, viele einst proprietäre Rundfunksysteme werden durch IT-Systeme abgelöst, man denke da zum Beispiel an Bandmaschinen, die immer mehr durch leistungsfähige Videoserver mit großen Festplattenspeichern ersetzt werden. In der Produktion erfolgen zahlreiche Bearbeitungsschritte auf handelsüblichen PCs. Immer mehr Zuspielungen erfolgen nicht mehr über Koaxialkabel und Kreuzschiene sondern über Ethernet- oder ATM-Netze, das gilt sowohl für hausinterne- wie für Zuspielungen von außerhalb (verteilte Produktion). Die Übertragungen können dabei als lineares Streaming (ASI über IP oder ATM) oder als nichtlinearer Filetransfer (TCP/IP) erfolgen.

Welche Risiken und Nebenwirkungen sollte man beachten? Die neuen IT-gestützten Systeme erleichtern den Workflow, bringen jedoch möglicherweise neue Risiken mit sich. Die sicheren Rundfunkprotokolle werden durch potentiell unsichere Protokolle ersetzt (TCP/IP, UDP). Auf PCs lauern zahlreiche unbekannte Risiken durch fehlerhafte Software mit Sicherheitslöchern (man denke an die vielen bekannt gewordenen Sicherheitslücken des Internet Explorer oder Outlook). Häufig werden Viren und Würmer über tragbare Medien (USB-Sticks, Disketten) oder Notebooks eingeschleust. Durch das Zusammenwachsen der Netze unter verschiedenen Rundfunkanstalten, Anbindung von "Außenreportern", die ihre Beiträge über DSL einspielen sowie die zunehmende Vernetzung der Produktionsinseln steigt die Gefahr einer raschen Ausbreitung der Schädlinge auf zahlreiche Systeme. Dabei kann es zu Schäden wie Datenverlust oder Manipulation der Daten bis hin zum kompletten Ausfall der Systeme kommen. Prinzipiell kann jedes System (PC, Router, Switch) Ziel einer Attacke werden.

Eine zusätzliche Gefährdung von Produktions-IT stellt die Voraussetzung an einen bestimmten Softwarestand dar, die Hersteller der Applikationen "erlauben" keine Sicherheits-Patches oder Virenscanner auf ihren Systemen. Hinzu kommt, dass Produktions-IT (z.B. NLE) oft nur im Administrator Modus betrieben wird.

Nachdem wir nun einige potentielle Sicherheitsprobleme aufgezeigt haben, stellen wir uns die Frage: wie schützen wir uns als Rundfunkanstalt? Dazu fallen uns spontan folgende Fragen ein:

• Wo sind Rundfunknetze angreifbar? Die meisten Rundfunkanstalten haben für Zuspielungen Regionetze aufgebaut die als weitgehend sicher gelten, da es sich in der Regel um dedizierte Providernetze oder sogar um angemietete "dark fiber" Netze handelt und das Netzequipment von der Anstalt selber "gemanaged" wird. In vielen Häusern sind jedoch drahtlose Netze im Einsatz, teilweise ohne Wissen der Administratoren (es gibt kaum noch Notebooks am Markt ohne WLAN-Interface). Somit stellt sich die Frage: ist sichergestellt, dass alle drahtlosen Netze den Sicherheitsanforderungen ent-