

Dreamlab IT-Security Bulletin – August 2007

Aktuelle und zukünftige IT-Security Bedrohungen

Die «digitale Revolution» ist abgeschlossen und hat während der letzten 30 Jahre erheblich an Einfluss auf den wirtschaftlichen Erfolg oder Misserfolg gewonnen und die Arbeits- und Produktionslandschaft hin zur heutigen Informationsgesellschaft verändert. Die Sonnenseiten der gesteigerten und effizienteren Produktion, vereinfachten Abläufen, schnelleren Kommunikation usw., haben aber – wie viele Dinge im Leben – auch ihre Schattenseiten. Nicht richtig gepflegt und mit fehlendem Know-how, wird dieser Segen sehr rasch zu einem Risiko. Erst mit dem so genannten «Y2K», dem Millenniumswechsel, trat das Risiko der Abhängigkeit in das Bewusstsein der Unternehmen und obwohl 9/11 dieses Bewusstsein nochmals verstärkt hat, so ist in der breiten Bevölkerung die Sicherheit in der IT erst seit etwa ein bis zwei Jahren zu einem Thema geworden.

Wer kennt sie also nicht, die Frage nach der Sicherheit der eigenen IT und nach der aktuellen Bedrohungslage? Es ist die Frage, mit der auch Dreamlab Technologies bei den Gesprächen mit den Kunden am meisten konfrontiert wird. Aus diesem Grund haben wir uns entschlossen, eine eigene Einschätzung der aktuellen Situation zu veröffentlichen. Diese basiert einerseits auf unseren eigenen Forschungsergebnissen und andererseits auf den Untersuchungen internationaler Untersuchungsbehörden, Partnerinstitutionen und externer Fachexperten. Wir konzentrieren uns dabei auf die Fragestellung, mit der sich IT-Verantwortliche zurzeit konfrontiert sehen. Natürlich sind IT-Umgebungen sowie deren Sicherheitsdispositive so unterschiedlich wie die Unternehmen selber, deshalb ist der Inhalt dieses Dokumentes bewusst allgemein gehalten, ohne auf spezifische Produkte oder Applikationen einzugehen.

Mobile Daten erleichtern den Datendiebstahl

Datendiebstähle bei verschiedenen namhaften Unternehmen wie Boeing, Ernst & Young sowie dem US Department of Homeland Security, haben in der Zwischenzeit bei vielen Firmen die Problematik des Mobile Computing und der Datenverschlüsselung ins Bewusstsein gerückt. Laut dem CSI / FBI Security Survey 2006 verkörpert Mobile Data Theft mit 47%, direkt nach Virenangriffen, bereits die zweithäufigste Art von Angriffen. Die teilweise Verschlüsselung von mobilen Daten stellt heute bei vielen Instituten bereits gängige Praxis dar, der Trend deutet jedoch zur transparenten Verschlüsselung elektronischer Daten. Dies hat zur Folge, dass Verschlüsselungsvorgänge benutzerfreundlicher werden und in für Anwender bekannte Vorgänge integriert sind. Beispielsweise bieten aktuelle, moderne Betriebssysteme Festplattenverschlüsselungen an, die direkt in den Anmeldevorgang am Computer integriert sind.

Funkübertragungen ermöglichen Datenmanipulation

Funkbasierte Datenübertragung liegt immer noch im Trend. Zunehmende Mobilitätsbedürfnisse in den Bereichen Office, Warehouse und PoS lassen unterschiedlichste Lösungen in diesen Bereichen entstehen. Elektronisches Ticketing, Verkehrsleitsysteme und implantierte, autonom im Menschen arbeitende Medizinalinstrumente sind hier nur einige Beispiele. Obwohl das Transportmedium Funk nie präzise kontrolliert werden kann und somit als Shared-Medium betrachtet werden muss, tragen die meisten Sicherheitsdispositive diesem Fakt keine Rechnung. Oft definiert sich die Sicherheit bei Funklösung in der Verfügbarkeit von Analysegeräten. Data Sniffing und Manipulation von kabellosen Netzwerken sind Common Know-how, andere Lösungen wie beispielsweise Bluetooth sind schwieriger abzuhören oder zu manipulieren, jedoch ist auch dies für eine versierte Person realisierbar. Proprietäre Funksysteme innerhalb der Industrie sind oft unverschlüsselt und äusserst anfällig auf Data Reinjection und -Manipulation.

Ein Trend im Bereich Funkübertragung ist der Einsatz von RFID-Technologie. Diese ist vielerorts für den Einsatz in Pässen oder Tickets wie für die EURO 08 vorgesehen. Die neuen Pässe mit RFID enthalten biometrische Daten des Passinhabers im RFID-Chip und sollen somit fälschungssicher sein. Bürgerrechtsorganisationen weisen seit längerer Zeit auf die Unsicherheit dieser Technologie hin und haben auch schon konkrete Fälschungsszenarien nachgewiesen. Die Konsequenz des Diebstahls von biometrischen Erkennungsmerkmalen ist gravierend. So können beispielsweise von entwendeten Fingerabdrücken Attrappen angefertigt werden, die es erlauben, «fremde» Fingerabdrücke zu hinterlassen.

All-Over-IP – Rush Hour auf dem Datenhighway

Der Datenfluss über IP Netzwerke nimmt stetig zu und immer neue Technologien beanspruchen zusätzlichen Platz auf diesen Netzwerken. Diese übermäßige Vernetzung führt zu einer exzessiven Ausweitung der möglichen Angriffsvektoren. Der Ausfall eines Routers innerhalb eines Firmennetzwerkes hat heute bereits deutlich mehr Auswirkung als noch vor fünf Jahren. Ein einzelner, erfolgreicher Angriff bedeutet oft Zugriff auf weite Teile des Unternehmens. Durch VoIP nutzen auch Telefonanlagen und Konferenzsysteme dieselben Transportwege. Die Technologie ist – verglichen mit konventionellen Telefonnetzen mit jahrzehntelangen Entwicklungsphasen wie POTS oder ISDN – noch sehr jung und dementsprechend ist mit anfänglichen Schwierigkeiten zu rechnen. Viele Fragen wie Verschlüsselung, Authentifizierung oder Fälschungssicherheit wurden bei VoIP noch nicht nachhaltig gelöst.

Embedded Computing, Firmwarehacking – auch die digitalen Helfer sind nicht von Angriffen geschützt

Schutzmechanismen innerhalb Betriebssysteme steigen. Angriffe werden komplexer und instabiler. Bereits seit Ende 2005 ist ein zunehmender Trend zu Angriffen / Analysen innerhalb der verschiedenen Embedded Devices Umgebungen festzustellen. Dies aufgrund mangelhafter Schutzmechanismen und der grossen Verbreitung von Robotiksystemen, Steuerungen, Routern, Barcodescannern und autonomen Ticketingsystemen. Bereits wurde mehrere Male demonstriert, wie Embedded Devices modifiziert werden können, um beispielsweise sämtliche verarbeitenden Daten zu modifizieren. Das Resultat ist stark abhängig vom Einsatzgebiet des Gerätes, kann jedoch vom Infizieren von Downloads bis hin zur Manipulation geschäftsrelevanter

Daten reichen. Ein Beispiel für eine erfolgreiche Attacke ist der Angriff einiger Aktivisten aus Holland, denen es gelungen ist, die Wahlcomputer für die Parlamentswahlen zu manipulieren und sogar zum Schachspielen zu bewegen. Die Liste lässt sich beliebig verlängern mit Beispielen von manipulierten Routern oder Überwachungskameras etc.

Moderne Webapplikationen, leichte Beute für XSS-Attacken und SQL-Injections

Immer mehr Applikationen werden ins Web portiert, um diese über das Internet weltweit erreichen zu können. Diese Entwicklung ist nicht nur bei firmeninternen Applikationen zu beobachten, sondern auch B2B-Schnittstellen werden immer mehr in Form von Web-Services bereitgestellt. Interessant ist diese Entwicklung vor allem auch was die Sicherheit angeht. Zum jetzigen Zeitpunkt betreffen mehr als die Hälfte aller täglich gemeldeten Attacken Webapplikationen. Besonders der Web 2.0 und AJAX Hype spiegelt sich deutlich in der Anzahl Attacken wieder, da viel zu häufig unterschätzt wird welche Gefahren solche Applikationen mit sich bringen. Dies kann zum Beispiel durch das „WASC Web Application Security Statistics Project“ belegt werden, welches zeigt, dass etwa 85% aller Webapplikationen auf so genannte XSS Attacken anfällig sind und etwas mehr als ein Viertel auf SQL-Injections. Dass solche Angriffe äusserst kostspielig und imageschädigend wirken können, mussten auch etliche renommierte Unternehmen wie Google, Microsoft, MySpace etc. feststellen. Einzelne Web-Services mussten gar temporär vom Netz genommen werden, um die Schäden beheben zu können.

Offshoring – Interface Definitionen

Sparmassnahmen haben in vielen Firmen zur Suche nach neuen Lösungen und mit der Verlagerung der Produktion durch Outsourcing und Offshoring zu Einsparungen beim Personal geführt. Aus Sicht der Sicherheit und Qualität birgt diese Entwicklung neue und zusätzliche Gefahren und Probleme. Gerade Offshoring von Arbeiten in kulturell stark abweichende Länder benötigen ausgesprochen präzise Formulierungen von Schnittstellen, Erwartungen und Resultaten. Diese Interface Definition war und ist noch immer eines der herausforderndsten Qualitäts- und Sicherheitsprobleme, das durch Kultur und Sprachunterschiede noch verstärkt wird. Unterschiedliche Massstäbe in Ausbildung, Reporting und Produktionsqualität stellen ein Problem dar, das anvisierte Sparmassnahmen häufig verunmöglicht oder sich sogar gegenteilig auswirkt. Dies ist einer der Gründe,

wieso bereits einige namhafte Unternehmen ihre Offshore-Aktivitäten rückgängig gemacht oder in Regionen verlagert haben, wo die kulturellen Unterschiede weniger ins Gewicht fallen.

IT Demographie fördert Legacy Systeme

Als IT Demographie bezeichnen wir den Verlust von IT-Know-how bis zu dessen Aussterben. Die IT Demographie zeigt sich zunehmend in grösseren Firmen. Durch strategischen Wandel, Portfolio- oder den Personalabbau existieren zunehmend Legacy Systeme und Applikationen, welche für die Unternehmen soviel an Wichtigkeit verloren haben, dass dieses Wissen nicht mehr ausreichend gepflegt wird. Auch wenn diese Systeme nach wie vor in Betrieb und deren Funktionen geschäftskritisch sind und deshalb nicht ausgemustert werden, wird oftmals aus Kostengründen nichts in den Erhalt des Know-hows investiert. Somit werden solche Systeme zu einem ausgeprägten Sicherheitsproblem. Oft ist der Herstellersupport nicht mehr gewährleistet und Applikationspatches sind nur noch unzureichend verfügbar. Dies macht solche Systeme sowie deren Umfeld verwundbar und zu äusserst attraktiven Angriffszielen. Ein gutes Beispiel aus dem Netzwerkbereich stellt hier X.25 dar. Dieses Protokoll ist eine der ersten eingesetzten Techniken für globale Vernetzung und war hauptsächlich in den 1980ern und frühen 1990ern populär. Es wird immer noch eingesetzt und nur noch von wenigen Fachleuten verstanden oder gepflegt. Es spielt heute jedoch immer noch eine wichtige Rolle für Transaktionssysteme, wie sie bei Banken oder Telekommunikationsunternehmen im Einsatz sind.

Identitätsdiebstahl kann jeden treffen

Die digitale Identität, die jede Person und jede Firma repräsentiert, ist ein beliebter Fokus von technologischen Angriffen. Laut Bericht des amerikanischen Justizministeriums aus dem Jahre 2006 entstehen in den USA jährlich über 6.4 Milliarden USD Schaden durch Identitätsdiebstahl. Durch Manipulation und geschickte Verbreitung von Informationen platzieren sich Kriminelle innerhalb ihres Zieles und eignen sich hierzu die Identität einer andern Person oder eines anderen Unternehmens an. Das Problem des Data-Phishing ist nur die Spitze dieses ernst zu nehmenden Problems. Die elektronische Datenerfassung gehört zum Alltag und wir vertrauen ihr zunehmend. Tagtäglich hinterlassen wir unsere persönlichen Daten auf E-Commerce-Webseiten, bei Preisausschreibungen, bei Rabattaktionen, im E-Government und in elektronischen Diskussionsforen.

Dadurch machen wir uns immer verletzlich. Kürzlich machte ein Mail einer Berner Anwaltskanzlei die Runde, in dem zur Bezahlung einer offenen Rechnung aufgefordert wird. Auch hier handelte es sich um einen Fall von Identitätsdiebstahl. Verschärfend kommt in diesem Fall hinzu, dass sich im pdf-Anhang der so genannte StormWorm-Virus versteckt, welcher sich beim öffnen in Rechner einnistet, verändert und weiter verbreitet.

Komplexität der Security vs. Professionalisierung der Angriffe

Generell werden Angriffstechniken und Methoden gezielter eingesetzt als früher. Ziele werden bewusster ausgewählt und Exploits und Backdoors für das entsprechende Ziel entwickelt. Ein erkennen von zielgerichteten Angriffen ist mit handelsüblicher Antivirensoftware kaum möglich. Das nötige Sicherheitsdispositiv nimmt an Komplexität zu, sobald der Funktionsumfang oder Benutzerkreis ausgeweitet wird. Leider kann das Schutzsystem selbst derart komplexe Formen annehmen, dass es viele Unternehmungen nicht mehr korrekt einsetzen und/oder betreiben können. Angreifer reagieren zudem auf etablierte Sicherheitsmassnahmen und entwickeln neue Angriffsmethoden, um die neuen Gegenmassnahmen zu umgehen. So berichten beispielsweise renommierte Fachmagazine und Sicherheitsspezialisten in regelmässigen Abständen über neue Techniken, um Viren an Virenscannern vorbeizuschleusen. Zusammen mit der Professionalisierung der Angriffe findet auch ein Paradigmenwechsel statt. Während früher Computerangriffe hauptsächlich breit angelegt waren (bspw. War-Dialing in grossen Telefonnummernblöcken) sind diese heutzutage zielgerichteter. Ein weiterer Unterschied besteht in der Motivation: Während früher Angriffe hauptsächlich aus Spass und als Selbstbestätigung gestartet wurden, stecken heutzutage häufig kriminelle Absichten und Konkurrenten dahinter. So häufen sich in letzter Zeit die Berichte über Wirtschaftsspionage, bei der Sicherheitssysteme umgangen werden. Ein Beispiel hierfür ist der Angriff von SAP auf Software von Oracle. Verschiedene Medien (wie Focus oder Der Spiegel) berichteten über den Vorfall.

Scheinsicherheit wird zum Bumerang-Effekt

Viele der heute eingesetzten Schutzmechanismen sind nur bedingt effizient gegen moderne Angriffe. So zum Beispiel nutzt eine auf Netzwerkebene funktionierende Firewall nur wenig gegen Angriffe auf der Applikationsebene. Die Benutzer und Betreiber solcher Mechanismen fühlen sich

jedoch meist sicher, bis ihnen das Gegenteil bewiesen wird. Im Extremfall kann diese Scheinsicherheit dazu führen, dass andere Massnahmen, die effizienter wären, nicht oder nur mangelhaft durchgeführt werden. Neuerdings geraten aber genau diese Mechanismen in den Fokus von Angreifern. Dieser Trend wird sich wohl fortsetzen, da ein Sicherheitsmechanismus meist mit erhöhten Rechten agiert und bei einem erfolgreichen Angriff dem Hacker diese weitervererbt. Ein verwundbares Mail-Antivirentool würde somit vollen Systemzugriff als auch Zugriff auf die E-Mails bieten.

Ein weiterer Aspekt der Scheinsicherheit ergibt sich bei den Virenscannern. Gemäss einer Studie der Computerzeitschrift c't ist die Erkennungsrate bereits bei den bekannten Viren sehr unterschiedlich und variiert zwischen 60 und 99%. Deshalb kann der Virenschanner als Sicherheitsmechanismus sehr trügerisch sein und der Anwender wiegt sich in falscher Sicherheit.

Dreamlab Technologies AG

Dreamlab Technologies AG ist ein auf IT-Security spezialisierter Solution Provider. Seit 1997 führen wir High-End Sicherheitstests, Beratungen und Schulungen durch. Als Mitbegründer von ISECOM arbeitet Dreamlab Technologies AG nach dem OSSTMM-Manual, der heute wohl am meisten verbreiteten Methodik für umfassende Audits im Security-Bereich. Intensive Forschung, die Mitgliedschaft in internationalen Organisationen wie das W3C und die Zusammenarbeit mit externen Experten sowie technischen Fachschulen und Universitäten im In- und Ausland garantieren Dreamlab Technologies AG den Zugang zu den neuesten Erkenntnissen und Entwicklungen. Auch in der Ausbildung setzt Dreamlab Technologies AG auf akademische Partnerschaften und hat mit diversen Hochschulen entsprechende Studienprogramme für ihre Studierenden erarbeitet. Zudem wird neben den auf die individuellen Bedürfnisse der Unternehmen zugeschnittenen Ausbildung auch ein breites Programm an öffentlichen Kursen angeboten. Ein weiterer Tätigkeitsbereich von Dreamlab Technologies AG ist die Entwicklung wegweisender Standard-Technologien wie X-Forms und BackTrack und von innovativen, auf Kundenbedürfnisse zugeschnittenen Speziallösungen.

Autor:

Dreamlab Technologies AG
Monbijoustrasse 36
CH-3011 Bern
contact@dreamlab.net
<http://dreamlab.net>

Die Publikation dieses Artikels ist unter Angabe der Quelle und Zusendung eines Belegexemplars ausdrücklich gestattet.