Enterprise Threat Management

Statische Sicherheitstools sind passé

Die Sicherheitstools der vergangenen 10 bis 15 Jahre basieren vorwiegend auf statischen Mechanismen. Firewalls etwa sperren bestimmte TCP- oder UDP-Ports für den Datenverkehr, während Systeme zur Erkennung von Angriffen – IDS (Intrusion Detection Systems) genannt – schädliche Software anhand unveränderlicher Signaturen identifizieren.

Diese Tools wurden unter der Annahme konzipiert, dass der Anwender die Ergebnisse korrekt interpretieren und die Konfiguration der Tools dementsprechend laufend modifizieren würde. Auch wurde angenommen, dass der Anwender über die Sicherheitsgefahren Bescheid weiß und in der Lage ist, die Sicherheitsinfrastruktur richtig zu konfigurieren.

Beide Annahmen haben sich jedoch im Laufe der Zeit als falsch erwiesen. IT-Sicherheitsexperten sind oft zwischen zahlreichen Aufgabenbereichen hin- und hergerissen und müssen dennoch in der Lage sein, auf Notsituationen wie eine Vireninfektion oder eine kriminaltechnische Untersuchung eines PCs zu reagieren. Die IT-Sicherheitsexperten haben daher nicht genug Zeit, um ein einzelnes Tool genau zu überwachen oder dessen Konfiguration regelmäßig zu aktualisieren. Außerdem ist es unmöglich, sich Fachkenntnisse über die Installation beziehungsweise Optimierung jedes einzelnen Tools anzueignen.

Der statische Charakter der Sicherheitstools wird zudem in vielen Unternehmen durch die eingesetzten Prozesse weiter verstärkt. Beispielsweise muss zum Sperren eines neuen Ports bzw. das Aufheben einer bestehenden Portsperre in einer Firewall üblicherweise ein Antrag auf Änderung gestellt werden, was oft Tage dauern kann. Diese Prozesse machen es schwerer, schnell auf neue Bedrohungen zu reagieren.

Das Aufkommen dynamischer Bedrohungen

Sicherheitstools sind zwar nach

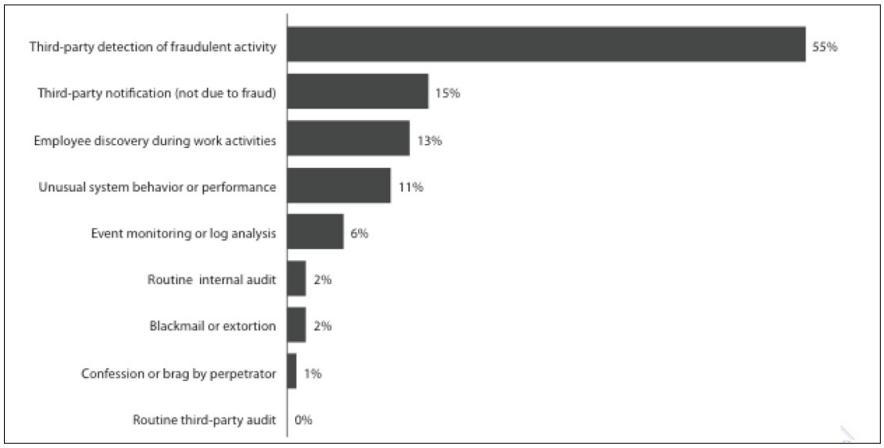
wie vor statisch, aber die Malware hat sich in den vergangenen Jahren bedeutend weiterentwickelt. Früher wurden Würmer und Viren von Computerfreaks geschrieben – heute werden sie in Forschungslabors mit kriminellen Absichten entwickelt.

Moderne Malware kann den statischen Schutz, den eine einfache Firewall oder ein einfaches IPS (Intrusion Prevention System) bietet, leicht umgehen. Eine Sperre bestimmter Ports ist oft ineffektiv, da die bösartige Software zur Verbindungsherstellung mit den Hostgeräten eine beliebige Anzahl von Ports dynamisch nutzen kann.

Darüber hinaus setzt die Malware unter Umständen diverse Verfahren zur Selbstmodifikation ein, um ihren Shellcode zu verbergen. Eine Suche nach statischen Angriffssignaturen liefert daher möglicherweise keine brauchbaren Ergebnisse.

Daher haben sich manche Sicherheitstools mit der Zeit weiterentwickelt, um mit den gegenwärtigen Bedrohungen fertigzuwerden. Snort von Sourcefire zum Beispiel ist ein IPS, das Angriffe moderner Malware erkennen kann. Das Snort-System modelliert spezifische Netzwerkprotokolle und ist mit deren Funktionsweise vertraut, so dass es potenzielle Sicherheitsverletzungen erfassen kann. Die Protokollmodellierung ermöglicht es, unabhängig vom eigentlichen Aussehen des Malware-Codes jeden potenziellen Exploit zu erkennen.

Selbst mit dieser Art von Intelligenz kann ein IPS allerdings so viele Daten liefern, dass es den IT-Sicherheitsexperten schwer fällt, die Situation richtig zu beurteilen. Eventuell verfügt das System nicht über den nötigen Kontext für eine korrekte Einschätzung.



Die Bedeutung von Kontext

Kontext bezieht sich auf die Fähigkeit, wichtige Umgebungsfaktoren verstehen und deuten zu können. Ein Spezialist für IT-Angriffe ist mit seinem Wissen über die Netzwerkumgebung und mit Kontextinformationen in der Lage, IPS-Warnmeldungen zu priorisieren und zu entscheiden, welche Warnmeldungen näher untersucht werden müssen.

Den meisten Unternehmen fehlt aber diese Art von Kontext. Laut einer 2009 von Verizon Business veröffentlichten Studie, bei der knapp 600 Datensicherheitsverletzungen der letzten fünf Jahre untersucht wurden, wurden 71 % der Sicherheitsverletzungen nicht von den betroffenen Organisationen, sondern durch Dritte, das Geständnis eines Täters oder im Rahmen eines unabhängigen Audits entdeckt (www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf (in englischer Sprache). Die betroffenen Organisationen hatten keine Ahnung, dass die Sicherheit ihrer Netzwerke beeinträchtigt war.

Eine weitere wichtige Erkenntnis der Studie ist, dass nur 6 % der Sicherheitsverletzungen intern durch eine Ereignisüberwachung oder Protokollanalyse entdeckt wurden.

Die Organisationen kaufen vielleicht Tools und setzen unter Umständen sogar Mitarbeiter zu deren Überwachung ein, aber solange diese nicht den korrekten Kontext zur Analyse der erhaltenen Daten haben, sind die Tools und Daten nur beschränkt von Nutzen.

Bei dynamischen Bedrohungen ist es wichtig, dass Unternehmen die Zusammensetzung der Hostgeräte in ihren Netzwerken und die auf diesen Hosts ausgeführten Anwendungen besser kennenlernen. Dieses Wissen liefert den nötigen Kontext, um die Warnmeldungen richtig zu priorisieren und die Bösartigkeit der Angriffe abschätzen zu können.

Echtzeit-Netzwerkinformationen

Sourcefire RNA (Real-time Network Awareness) nutzt ein passives Erkennungsverfahren, das bei der täglichen Analyse von Eindringversuchen behilflich sein soll. RNA überwacht den Netzwerkverkehr in Echtzeit und zeichnet Änderungen in der Hostkonfiguration sowie das Netzwerkverhalten der Hosts auf. Da RNA passiv arbeitet, bietet es gegenüber herkömmlichen Netzwerküberwachungsverfahren, die auf aktiven Scans oder hostbasierten Agenten beruhen, einige Vorteile:

- Es verursacht keinen Datenverkehr, der Bandbreite beanspruchen oder die Netzwerkinfrastruktur beeinträchtigen kann.
- Es liefert eine Echtzeitansicht des Netzwerks, die laufend aktualisiert wird, wenn Geräte Daten durch das Netzwerk schicken – die Daten sind nie veraltet und nicht von regelmäßigen, aktiven Scans abhängig.
- Es ist nicht von auf Endgeräten installierten Agenten abhängig, die betreut werden müssen – unbekannte oder nicht autorisierte Geräte sind immer sichtbar.

RNA weist eine Reihe von für die Angriffsanalyse äußerst relevanten Funktionen auf. Es liefert Kontextinformationen über das Netzwerk und verringert die Anzahl der festgestellten Eindringversuche, die eine Maßnahme erfordern, beträchtlich. Darüber hinaus setzt RNA seine Netzwerkinformationen zur automatischen Anpassung von Sourcefire IPS ein, was den Arbeitsaufwand senkt und die Systemleistung steigert.

Weniger Angriffswarnmeldungen

Das System nutzt seine passive Technologie, um Informationen über die Netzwerkkomponenten zu erfassen. Auf Grundlage dieser Daten wird dann ein Netzwerkplan mit allen Hostgeräten inklusive Betriebssystem, Anwendungen und potentiellen Schwachstellen erstellt. Das Programm zieht diese Daten heran, um die möglichen Auswirkungen von Eindringversuchen nach ihrer Priorität einzustufen.

Das IPS klassifiziert so Angriffe auf das Netzwert. Der Sicherheitsexperte kann sich so dann darauf konzentrieren, nur die als „Gefahr" gekennzeichneten Ereignisse näher zu untersuchen, und die als „Keine Gefahr" identifizierten Ereignisse außer Acht lassen. Die Auswirkungsanalyse kann die Anzahl der Ereignisse, die Maßnahmen erfordern, um das 10- bis 100-fache reduzieren. RNA liefert dem Sicherheitsexperten den nötigen Kontext, um zu entscheiden, ob ein Eindringversuch wirklich näher untersucht werden muss, so dass er mehr Zeit für andere Aufgaben hat.

Automatische IPS-Anpassung – „Adaptives IPS"

Zur Anpassung von Sourcefire IPS nutzt RNA eine Funktion namens RRR („RNA-Recommended Rules"). Da RNA weiß, welche Betriebssysteme und Dienste im Netzwerk ausgeführt werden, kann RRR empfehlen, nur die relevanten Snort-Regeln anzuwenden. Wenn RNA beispielsweise feststellt, dass ein geschütztes Netzwerksegment nur Linux-Systeme mit Unterstützung für Webservices und NIS aufweist, kann RNA empfehlen, sämtliche für Windows-Hosts und Dienste wie etwa IIS geltende Regeln außer Acht zu lassen. RRR wurde dafür konzipiert, die Schutz- und Erkennungsleistung zu maximieren und den erforderlichen Aufwand zur laufenden manuellen Anpassung von Sourcefire IPS beträchtlich zu verringern bzw. nahezu ganz zu beseitigen. Regelempfehlungen von RRR können mit oder ohne Benutzereingriff implementiert werden.

RNA unterstützt auch andere automatische Anpassungsverfahren. Eine weitere Anpassungsfunktion des adaptiven IPS untersucht den Datenverkehr über nicht standardmäßige Ports und trägt so dazu bei, ein mögliches Umgehen des IPS zu verhindern. Ein Nutzer könnte beispielsweise versuchen, seinen HTTP-Datenverkehr zu verbergen, indem er anstelle des standardmäßigen TCP-Ports 80 den TCP-Port 8888 verwendet. Herkömmliche IPS-Anwendungen können diesen Datenverkehr zwar erfassen, liefern aber für gewöhnlich eine suboptimale Leistung oder erfordern eine manuelle Konfiguration der Regeln für nicht standardmäßige Ports. Im Gegensatz dazu kann RNA die Ports und Dienste auf den überwachten Hostgeräten identifizieren und das IPS so konfigurieren, dass immer die korrekten Regeln für nicht standardmäßige Ports angewendet werden.

Zusammengefasst lässt sich sagen, dass die automatischen Anpassungsverfahren von RNA mehrere Vorteile mit sich bringen:

1. Weniger manueller Aufwand bei der Anpassung von IPS-Systemen.
2. Besserer Schutz vor Versuchen, das IPS zu umgehen.
3. Maximale Ausnutzung der Erkennungsressourcen.

Schlussfolgerung

Viele Unternehmen arbeiten immer noch mit statischen Sicherheitssystemen, die in einer früheren Ära entwickelt wurden. Sie verfügen nicht über die nötigen Mittel, um die heutzutage so häufigen dynamischen Bedrohungen abzuwehren. Die IT-Sicherheitsexperten sind mit ihren zahlreichen Aufgaben überlastet und müssen sich auf ein automatisiertes System verlassen, das ihnen Kontext zur Verfügung stellt und dabei hilft, echte Bedrohungen vom restlichen Datenverkehr zu unterscheiden. Sourcefire RNA liefert IT-Sicherheitsexperten diesen Kontext und hilft ihnen dabei, die Absicherung der IT-Infrastruktur ihres Unternehmens zu automatisieren.

Wolfgang Hustädt,
Security Engineer, Sourcefire

„Das Snort-System modelliert spezifische Netzwerkprotokolle und ist mit deren Funktionsweise vertraut, so dass es potenzielle Sicherheitsverletzungen erfassen kann. Die Protokollmodellierung ermöglicht es, unabhängig vom eigentlichen Aussehen des Malware-Codes jeden potenziellen Exploit zu erkennen."

Wolfgang Hustädt,
Security Engineer D A CH
bei Sourcefire

Datenschutz ohne Grenzen

Vorgehensmodell für den Datenschutz bei Offshoring-Projekten

Nicht erst seit jüngsten Presseberichten über Datenschutzpannen hat sich wirksamer Datenschutz zu einer wichtigen Voraussetzung unternehmerischen Erfolgs entwickelt.

Gerade für Firmen, die Massenkundendaten verarbeiten, wie etwa Telekommunikationsunternehmen, Banken oder auch Versandhändler, ist der sichere und zuverlässige Umgang mit Namen, Anschriften oder Nutzungs- beziehungsweise Verhaltensdaten unerlässlich. „Datenschutz" stellt hierbei den allgemein gebräuchlichen Begriff für die Verhinderung des Missbrauchs personenbezogener Daten dar.

Offshoring als globaler Megatrend

Die strikte Einhaltung der Datenschutzvorgaben wird insbesondere dann zu einer komplexen Aufgabe, wenn die IT oder IT-bezogene Dienstleistungen ins Ausland verlagert werden. Dieser Trend im Rahmen der Globalisierung, auch „Offshoring" genannt, hat sich in vielen Fällen als wirtschaftlich lohnend herausgestellt. Geringere Arbeitskosten stellen die in der Regel maßgebliche Motivation dar. Gerade Großunternehmen lagern wesentliche Teile ihrer IT aus, beispielsweise nach Osteuropa, Indien oder Ostasien.

Verantwortlichkeiten

Die Sicherstellung hohen Datenschutzes ist eine notwendige Bedingung erfolgreichen Offshorings. Schließlich soll auch dann ein hohes Datenschutzniveau gewährleistet sein, wenn IT-Entwicklung, -Betrieb oder -Support nicht mehr innerhalb deutscher oder gar europäischer Grenzen stattfindet. Bild 1 zeigt die offshore, also im Ausland einzuhaltenden fundamentalen Vorgaben des Bundesdatenschutzgesetzes (BDSG).

Es belegt, dass die gesetzlich geforderte Beurteilung des Schutzniveaus als „angemessen" von einer Vielzahl von Faktoren abhängt. Die Art der Daten beispielsweise, etwa Adress- oder Logindaten, beeinflusst diese Beurteilung. Gleiches gilt für die Zweckbestimmung der Daten, die zum Beispiel Test- oder Produktivbetrieb lauten kann. Die Zuständigkeit für die Einhaltung dieses Niveaus hingegen ist eindeutig geregelt: Das auslagernde Unternehmen muss hinreichenden Datenschutz sicherstellen; es ist dafür verantwortlich, dass auch offshore deutsche Datenschutzstandards eingehalten werden. Dies ist besonders schwierig, da lokale Rechtsbestimmungen und Gewohnheiten für die ausländischen Arbeitskräfte prägend, deutsche Standards hingegen in der Regel nicht bekannt sind.

Bild 1: Gesetzliche Vorgaben des BDSG zum Offshore-Datenschutz. (Bilder: Arkadia)

Bild 2: Systematische Vorgehensweise zur Sicherstellung des Offshore-Datenschutzes.

Datenschutzverletzung in Offshore-Projekten

Arkadia Management Consultants hat international agierende Unternehmen bei der Sicherstellung hohen Datenschutzes an Offshore-Standorten begleitet. Die Erfahrung zeigt, dass ein Großteil der IT-Anwendungen im Offshoring den Vorgaben zur Datensicherheit nicht entspricht. Dabei ist es unerheblich, ob die Daten tatsächlich übermittelt werden oder ob lediglich eine Möglichkeit des Datenzugriffs vom Offshore-Standort besteht. Die Risiken sind immens: Entweder werden erhebliche Maßnahmen zur Sicherung des Datenschutzes oder aber millionenschwere Rückverlagerungsprogramme notwendig. Für viele Unternehmen ergibt sich daher Handlungsbedarf.

Wie aber kann Datenschutz sichergestellt werden, wenn sich das Schutzobjekt – die Daten – in großer geographischer Distanz, in der Obhut unvertrauter Personen und damit offenbar fernab jeglicher Kontrollmöglichkeit befindet?

Vorschlag eines systematischen Vorgehensmodells

Arkadia hat ein in der Praxis erprobtes Vorgehensmodell zur Herstellung dauerhaften Offshore-Datenschutzes entwickelt (vgl. Bild 2): Zunächst ist die grundsätzliche Schutzbedürftigkeit festzustellen (Schritt 1). Anschließend erfolgt die Datenschutzprüfung (Schritt 2). Sofern ihr Resultat die Unzulässigkeit des Offshorings ausweist, muss durch gezielte Maßnahmen das geforderte Schutzniveau erreicht werden (Schritt 3). Das dauerhafte Sicherstellen dieses Niveaus ist das Ziel des finalen Prozessschritts (Schritt 4).

Schritt 1: Feststellung der Datenschutzbedürftigkeit

Zur Feststellung der Schutzbedürftigkeit der Daten ist eine Analyse der datenschutzbezogenen Situation vorzunehmen. Die Praxis zeigt, dass die Bestimmung des Status quo eine mitunter hohe Komplexität der IT- und Datenverarbeitungsstrukturen zu Tage fördert und daher mit einem nicht zu unterschätzenden Aufwand einher geht. Doch nur auf Basis einer detaillierten Analyse des Ist-Zustandes kann abgeleitet werden, welcher Handlungsbedarf zur Sicherstellung ausreichenden Datenschutzes besteht. Bild 3 zeigt die vier charakteristischen Inhalte dieser Analyse.

Bild 3: Inhalte der Analyse des Status Quo.

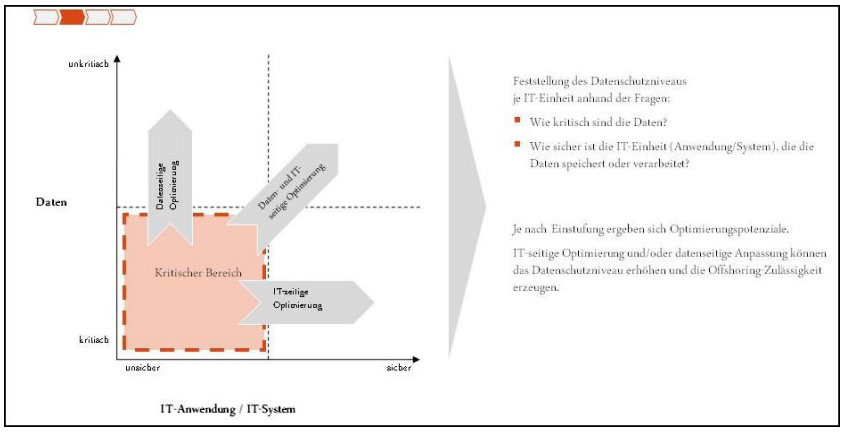


Bild 4: Schemenhafte Einstufung von Daten und IT nach Durchführung der Datenschutzprüfung.

Es illustriert, dass die Datenverarbeitung einem datenschutzrechtlich vorgegebenen Rahmen genügen muss. Aus diesem ergibt sich die Schutzbedürftigkeit der Daten. Darauf basierend ist zu ermitteln, inwieweit die datenschutzrechtlichen Anforderungen eingehalten werden. Dies ist Aufgabe der eigentlichen Datenschutzprüfung.

Schritt 2: Offshoring-Datenschutzprüfung

Die Datenschutzprüfung gibt Aufschluss darüber, welches Niveau der Datenschutz in einem Offshoringvorhaben aufweist. Sie besteht aus einer gesetzlichen Prüfung sowie dem unternehmensspezifischen Offshoring Audit.

Die gesetzliche Prüfung, auf die hier nur kurz eingegangen werden soll, wird in zwei Stufen vollzogen: Zunächst muss jedes Unternehmen, das Daten übermittelt, klären, ob die Übermittlung zulässig ist. In der zweiten Stufe muss geklärt werden, ob die von der Übermittlung betroffenen Personen durch die Weitergabe ihrer Daten keine unverhältnismäßigen Eingriffe in ihre Persönlichkeitsrechte erleiden. Wird bei dieser Prüfung ein nicht angemessenes Niveau festgestellt und greifen auch die Ausnahmen des BDSG nicht, muss das übermittelnde Unternehmen den Schutz des Persönlichkeitsrechts der Betroffenen garantieren. Hierzu bietet die Europäische Union Standardverträge sowie Vorgaben zur individuellen Vertragsgestaltung zwischen den datenübermittelnden und -empfangenden Stellen.

Das Offshoring Audit ist ein unternehmensspezifischer Check der Eignung zum Offshoring. Dieser wird je datenschutzrelevantem IT-System durchgeführt. Die fachlich Verantwortlichen müssen hierzu ihre Detailkenntnis über das jeweilige IT-System und die darin verarbeiteten Daten an die unternehmensinternen Datenschutzexperten berichten. Dies erfolgt mittels einer strukturierten Befragung. Dadurch wird eine detaillierte Erfassung der Verarbeitung kritischer Daten sichergestellt.

Neben den Daten muss auch die betroffene IT explizit der Analyse unterzogen werden. Schließlich ist zu prüfen, inwieweit Systeme oder Applikationen zum Schutz der durch sie verarbeiteten Daten beitragen.

Auf Basis der zusammengetragenen Informationen fällen die Datenschutzexperten ihr Urteil über das Schutzniveau der Daten beziehungsweise der IT, mit der die Daten verarbeitet werden (Bild 4). Auf Basis des in Bild 4 schemenhaft dargestellten Prüfungsergebnisses wird, in Einklang mit den Ergebnissen der gesetzlichen Prüfung, ein Urteil über die Zulässigkeit des Offshorings erteilt. Fällt dieses negativ aus, sind Anpassungsmaßnahmen zwingend erforderlich. Diese erfolgen im dritten Schritt der empfohlenen Vorgehensweise.

Schritt 3: Herstellung des geforderten Datenschutzniveaus

Zur Herstellung der Offshore-Zulässigkeit von Daten müssen für die betroffenen IT-Anwendungen Optimierungsmaßnahmen umgesetzt werden. Je nach Diskrepanz

zwischen gefordertem und tatsächlichem Schutzniveau ist aus einem breiten Spektrum von Maßnahmen zu wählen. Bild 5 zeigt die grundsätzlich bestehenden Handlungsoptionen auf.

Durch technische Maßnahmen werden die Daten selbst „unschädlich" gemacht. Diese Maßnahmen können jedoch nur nach eingängiger Prüfung der Daten sowie der entsprechenden IT umgesetzt werden, schließlich soll der betroffene Geschäftsprozess trotz des Eingriffes ohne Einschränkungen

Bild 5: Empfohlene Handlungsoptionen zur Sicherstellung der Offshoring-Zulässigkeit.

fortbestehen. Additiv umzusetzende nicht-technische Maßnahmen hingegen lassen die Daten selbst zunächst unberührt und zielen stattdessen auf Anpassungen im Umgang mit den Daten ab. Herausforderungen liegen hierbei in Auswahl und Sensibilisierung der Mitarbeiter und externen Partner sowie in der Sicherstellung der Vertragseinhaltung. Als letzter Ausweg bleibt als nicht-technische Maßnahme die mitunter teure Rückverlagerung nach Deutschland („Backshoring").

Die Notwendigkeit einer nachträglichen Herstellung der Offshore-Zulässigkeit sollte natürlich vermieden werden. Um sie konsequent auszuschließen, dürfen Manager Datenschutz nicht als einmalig durchzuführendes Projekt ansehen. Stattdessen sollten sich Unternehmen diesem Thema permanent mit der ihm zustehenden Aufmerksamkeit widmen.

Schritt 4: Dauerhafte Sicherung des geforderten Datenschutzniveaus

Datenschutz ist dauerhaft zu garantieren. Die kurzfristige Bereinigung von Sicherheitslücken und -schwachstellen kann dazu nur ein Anfang sein. Vielmehr muss, ausgehend vom Management, ein deutliches Bekenntnis zur Einhaltung der Datenschutzanforderungen abgegeben werden.

Ferner sind wichtige inhaltliche Weichenstellungen zu vollziehen. Es ist zu klären, wodurch Anpassungsmaßnahmen zur dauerhaften Einhaltung des geforderten Datenschutzes überhaupt notwendig werden. Hierbei gilt der Fokus den vier zur Ermittlung der Schutzbedürftigkeit dokumentierten Aspekten (siehe Schritt 1): Daten, IT-bezogener Rahmen, organisatorischer und geographischer Rahmen sowie datenschutzrechtlicher Rahmen.

Rechtliche oder datenseitige Modifikationen sind, genau wie organisatorische bzw. geographische Umstellungen, relativ leicht zu erfassen. Daher eignen sie sich gut für eine regelmäßige Überwachung (Monitoring). Die in der Praxis häufigste und datenschutzrechtlich wohl anspruchsvollste Ursache für geänderte Schutzbedürftigkeit sind Neuerungen der IT. Aktualisierungen und Erweiterungen bestehender Systeme sowie die Integration neuer Systeme dienen der Optimierung der Geschäftsprozesse und damit der Erreichung der unternehmerischen Ziele. Die Herausforderung besteht darin, rechtzeitig zu erkennen, ob IT-Änderungen die Schutzbedürftigkeit beeinflussen. Ist dies der Fall, muss die Einhaltung des geforderten Schutzniveaus geprüft werden. Erst dann kann über den Fortbestand des bisherigen Urteils über die Offshore-Zulässigkeit entschieden werden. Es ist daher notwendig, die IT-Entwicklung organisatorisch mit dem Datenschutz zu verknüpfen. So kann gewährleistet werden, dass Weiterentwicklungen der IT auch hinsichtlich ihrer datenschutzrelevanten Auswirkungen berücksichtigt werden.

Datenschutz planvoll angehen

Jedes Unternehmen, das Offshoring betreibt, sollte sich das Niveau seines Datenschutzes permanent explizit bewusst machen, bevor ernsthafte Pannen im Umgang mit kritischen Daten auftreten. Der empfohlene Prozess ist in der Praxis erprobt. Das Thema Datenschutz wird durch ihn planvoll adressiert, das Risiko unzureichenden Datenschutzes erheblich gesenkt. Dies rechtfertigt auch die Investition, die mit der Implementierung eines derartigen Prozesses verbunden ist. Die Erfahrungen zeigen, dass ein konsequent aufgebauter Datenschutz schnell Erfolge vorweisen kann: Die Lernkurve steigt steil an, sodass die Kosten zur Aufrechterhaltung des Schutzniveaus im Zeitverlauf stark abnehmen. Hinzu kommt die positive Wirkung des verantwortungsvollen Umgangs mit sensiblen Daten. Ist der Datenschutz – auch durch IT-Unterstützung – gewährleistet, entlastet dies nicht nur die Mitarbeiter. Auch die Außendarstellung der Organisation kann davon erheblich profitieren.

Markus Stratmann
markus.stratmann@arkadia.de

Florenz Lammert
Florenz.lammert@arkadia.de

Quantensprung

Die Quantifizierung von Informationssicherheit

Für die meisten Mitarbeiter in Unternehmen bedeutet Sicherheit ein muskelbepackter Wachmann, eine elektronisch gesicherte Eingangstür, die das Durchziehen eines Sicherheitsausweises verlangt, oder vielleicht noch eine Firewall auf dem Arbeitsplatzrechner.

Für Prof. Dr. -Ing. Clemens Martin von der Dualen Hochschule Baden Württemberg in Mannheim bedeutet Sicherheit jedoch viel mehr. Als Experte im Bereich Betriebssysteme und Netzwerke weiss er natürlich um den Wert der auf Computern gespeicherten Daten und sein Forschungsfeld an der DHBW dreht sich darum die Sicherheitsverfahren und Systeme zu verbessern, die die unternehmenskritischen Daten und Informationen schützen.

Als Professor der Wirtschaftsinformatik in der Fakultät für Betriebswirtschaft der DHBW vereint Prof.Dr.-Ing. Martin präzise akademische Arbeit mit umfangreicher Erfahrung im wirtschaftlichen Umfeld: „Informationen, die Unternehmen sammeln, neu schaffen und wieder verbreiten gehören

zu deren wertvollsten Gütern“ konstatiert Prof.Dr.-Ing. Martin.

Die Gründe Hackern und auch Wettbewerbern jeweils einen Schritt vorausbleiben zu wollen, sind klar. Allein in den USA verursachten Verletzungen der IT Sicherheit bei den Unternehmen Kosten im Durchschnitt pro Vorfall von $234.000 (CSI Report 2009); eine Zahl, die zwar unter der des Vorjahres aber immer noch oberhalb der von 2005/2006 erhobenen Werte liegt. Spitzenreiter (mit $770.000) sind mittlerweile Sicherheitsvorfälle, die auf Schwächen in der Wireless-Infrastruktur basieren (vor Diebstahl von mobilen Geräten mit $710.000 und finanziellem Betrug mit $450.000). Prozentual gesehen liegen die Vorfälle die durch Infektionen mit Schadsoftware verursacht wurden, mit 64,3 % deutlich vor den Diebstählen von Laptops und anderen mobilen Geräten (42,2%) und den in 2007 mit fast 60% noch an der Spitze liegenden „Insider“-Attacken (29.7%).

„Mein Hauptfokus liegt auf Informationssicherheitsbetrachtungen für die Unternehmensebene, nicht im Detail der technischen Infrastrukturlösungen, sondern auf den Technologien und Methoden die eine bessere Unterstützung der Geschäftsprozesse erlauben“, so Dr. Martin.

Die Ermittlung von geschäftsrelevanten Informationssicherheitsinformationen wird zunehmend wichtiger. In Folge der Finanzskandale in den USA rund um Enron und WorldCom sind dort mit der Sarbanes-Oxley Gesetzgebung von 2002 Auflagen für die Industrie geschaffen worden, die mittlerweile entsprechende oder ähnliche Maßnahmen in der gesamten industrialisierten Welt nach sich gezogen haben. Das ursprüngliche Gesetz verlangt, dass börsengelistete Unternehmen in ihren Jahresberichten über die Effektivität ihrer internen Kontrollsysteme für die finanzbuchhaltenden Systeme Auskunft geben.

„Für die Unternehmen, die Audits durchführen und Jahresabschlüsse prüfen, stellt dies eine Herausforderung dar, weil ihr Prüfungsauftrag nun so verstanden wird, dass auch die Prozesse und Systeme zur Gewährleistung der Unverfälschtheit und zum Schutz dieser Finanzdaten mitgeprüft werden müssen“, sagt Dr. Martin. „Sicherheitsmechanismen sind notwendig um die Kompromittierung dieser Daten wirkungsvoll zu verhindern. Für das obere Management stellt sich in Folge dessen allerdings die schwierige Frage, wie genau es um die Informationssicherheit in ihren Unternehmen steht und in welcher Qualität diese gemanaged wird. Gerade im Hinblick auf unliebsame Überraschung bei den entsprechenden Unternehmensprüfungen möchte man vorbereitet sein, um proaktiv handeln zu können.“

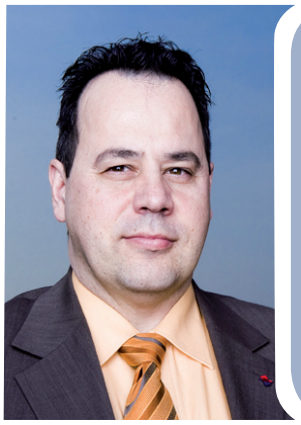
In seinem bereits an seiner vorigen Universität, der University of Ontario Institute of Technology (UOIT) in Kanada, in Zusammenarbeit mit Bell Canada, der größten kanadischen Telefongesellschaft, begonnenen Forschungsvorhaben versucht Dr. Martin effizientere Methoden zu entwickeln, um Unternehmen besser und schneller Auskunft über den Status der Informationssicherheit geben zu können.

„Viele informationstechnisch orientierten Überlegungen für große Systeme beschränken sich auf Fragestellungen wie ‘Woher bekomme ich welche Daten und wie verarbeite ich diese möglichst effizient?’, wie sie etwa von Security Information Management Systemen beantwortet wird. Dabei wird häufig die Frage des gesamtunternehmerischen Zusammenhangs und damit der Unterstützung der Unternehmensziele außer Acht gelassen. Seine Forschungsarbeiten konzentrieren sich daher auf die Entwicklung eines ‘Information Security Dashboards‘ für die Managementebene, um damit eine effizientere Erfolgskontrolle und Ressourcensteuerung zu ermöglichen. Letztendliches Ziel ist es, ein Informationssicherheits-Regelungssystem zu entwerfen, das das Management bei der Auswahl geeigneter Maßnahmenpakete unterstützt.“

Kenntnis um die Bedrohungslage und die damit verbundenen Sicherheitsvorfälle ist eines der Themen mit denen er sich auch mit seiner Co-Autorin Dr. Bernadette Schell, ehemalige Dekanin der Fakultät für Business & IT an der UOIT, in zwei Büchern „Cybercrime“ und dem „Webster›s New World Hacker Dictionary“ intensiv beschäftigt hat.

„Die ‚Bad Guys‘ verbessern kontinuierlich ihre Kentnisse und Methoden“, sagt er offen. „Wir müssen sicherstellen, dass die ‚Good Guys‘ nicht auf der Verliererseite landen“.

Nach der Entwicklung des ersten kanadischen Masters of IT Security hat Dr. Martin nun für die Duale Hochschule Baden Württemberg in Mannheim den MBA-Studiengang „IT Management“ entwickelt. Dieser weist als eine von drei möglichen Vertiefungsrichtung das „Management von Informationssicherheit“ auf und wird unter Leitung von Dr. Martin ab September 2010 durch die Graduate School Rhein-Neckar, den Kooperationspartner der DHBW Mannheim für weiterführende und berufsbegleitende Studiengänge, angeboten.



„Für die Unternehmen, die Audits durchführen und Jahresabschlüsse prüfen, stellen die neuen gesetzlichen Vorgaben eine Herausforderung dar, weil ihr Prüfungsauftrag nun so verstanden wird, dass auch die Prozesse und Systeme zur Gewährleistung der Unverfälschtheit und zum Schutz dieser Finanzdaten mit geprüft werden müssen.“

Prof. Dr.-Ing. Clemens Martin

itsecurity

Heft 4-2010 Juli /August erscheint am 28.6.2010

Anzeigenschluss für die nächste Ausgabe: 7.Juni 2010

VOIP Gefahrenpotenziale

Die IP-Telefonie, kurz VoIP, wirbt mit neuen Möglichkeiten der kostengünstigen Kommunikation. Das stimmt zwar, aber die Integration von Daten- und Sprachnachrichten in einem gemeinsamen Kanal birgt leider aber auch zahlreiche Risiken. Denn die Gefahren, die beim Telefonieren über das Internet auftauchen können, sind im Prinzip die gleichen, die beim normalen Internetbetrieb lauern. Verstopfte Mailboxen sind zwar ein Ärgernis, aber Spoofing mit dem über fremde Server telefoniert und Gespräche abgehört werden, sind neue, reale Gefahrenpotenziale. Aber auch fehlende Zugangskontrollen machen den Unternehmen zu schaffen. Da hilft nur ein Risikomanagement, um die Gefahren zu antizipieren und in den Griff zu bekommen.

Kryptografie

Das Knacken von asymmetrischen Verschlüsselungstechniken mit einer Schlüssellänge über 512 Bit ist im Moment unmöglich, da es rechnerisch und somit zeitlich viel zu aufwendig ist. Aber was ist heutzutage schon sicher? Wir berichten über die aktuellen Trends.

Virenschutzsoftware

Jeder Hersteller ist der größte, beste, schnellste, erfolgreichste Virenjäger. „Much ado about nothing", hieß es schon bei Shakespeare. Auf dem Markt gibt es dazu zahllose Antiviren- und Sicherheitslösungen mit unterschiedlichen Schwerpunkten und Zielgruppen. Wie soll man da die passenden Software für das Unternehmen auswählen? Es bietet sich an, die ebenso zahllosen Vergleichstests von Schutzsoftware als Entscheidungshilfe zu nutzen. Nur helfen die Vergleichstests auch wirklich die passende Schutzsoftware zu finden? Was steckt eigentlich hinter diesen Tests. Wer macht sie? Und warum?

Weitere Themen:

- RZ-Sicherheit
- Security Benchmarking
- Rethink Remote Access
- Enterprise Threat Management

hakin9

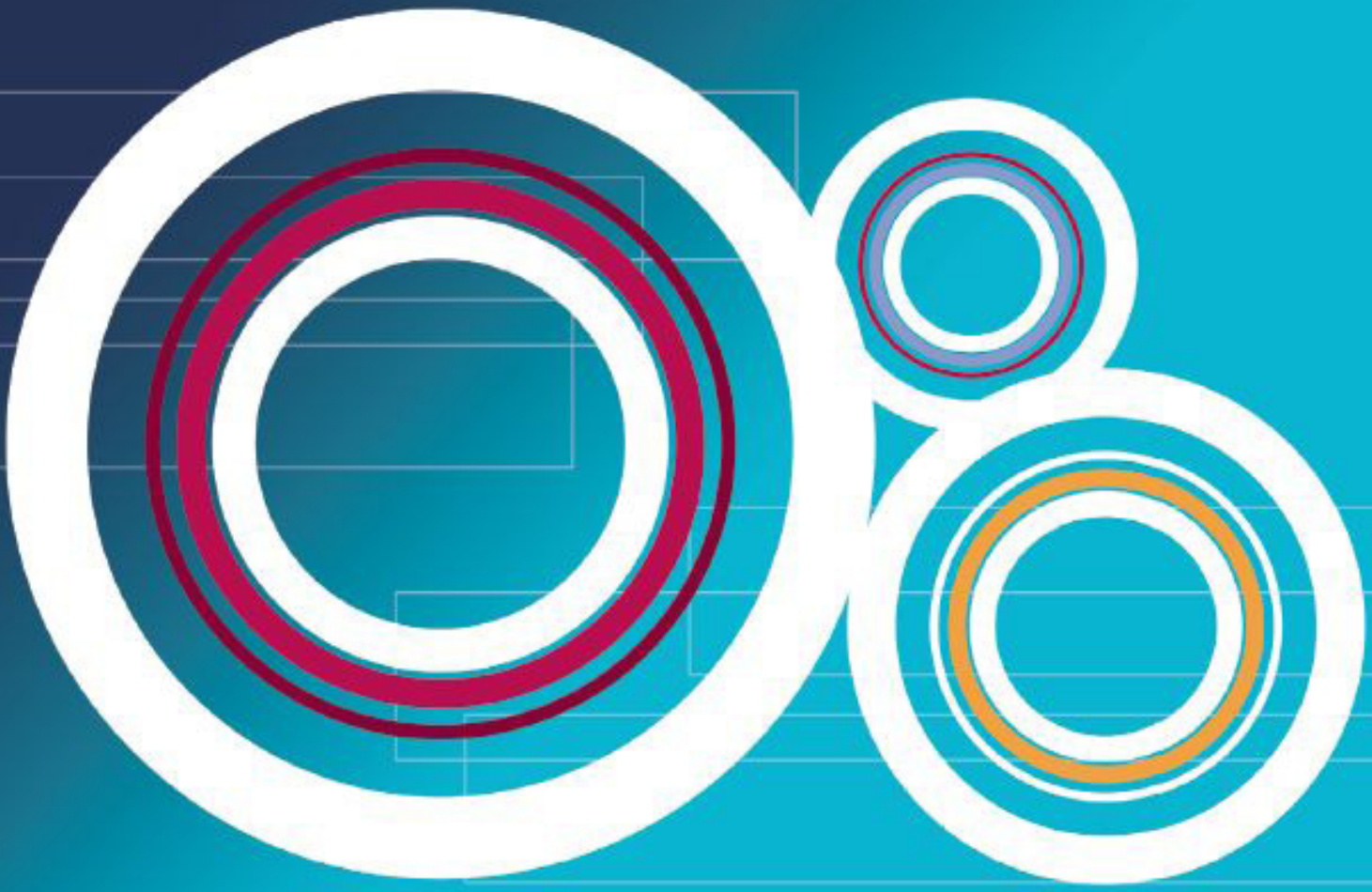
HARD CORE IT SECURITY MAGAZINE

Wir machen Sie mit der IT-Sicherheit vertraut!

Besuchen Sie unsere Website: www.hakin9.org/de
Artikel zum kostenlosen Download und mehr...

Unser Schnupperangebot: 3 Probehefte zum Preis von 23,50 €
Bestellungen an: abo@software.com.pl

PROJEKT MANAGEMENT 2010



Optimize Your IT Projects

Konferenz: 18. bis 19. Mai 2010

itverlag itevents

www.pmkonferenz.de