Botnetze
Ungewollte Unternehmensübernahmen

Längst stellen Botnetze nicht mehr nur eine Gefahr für den Heim-PC dar. Die Gefahr für Unternehmen, Ziel von Botnet-Attacken zu werden, steigt an.

Farbenfroh und friedlich – unter Naturliebhabern genießt der Schmetterling eine große Aufmerksamkeit. Den unangenehmsten aller Schmetterlinge jagten Behörden und IT-Spezialisten jedoch über ein Jahr lang, um ihn unschädlich zu machen. Im März 2010 wurde das Botnetz Mariposa (spanisch für Schmetterling) abgeschaltet und die Botmaster – drei Spanier im Alter zwischen 25 und 31 Jahren – verhaftet. Ihnen war es gelungen, Millionen Rechner in 190 Ländern zu infizieren, darunter Maschinen von mehr als der Hälfte aller amerikanischen Fortune 1.000-Unternehmen und rund 40 Großbanken. Diese erschreckende Bilanz von Mariposa lässt keinen Zweifel: Auch für Unternehmen bergen Botnetze ein immer größeres Gefahrenpotential.

Botnetze und ihre Strukturen

Botnetze (engl. Botnets) sind Netzwerke von kompromittierten Maschinen, die unter der Kontrolle eines Angreifers stehen. Der Angreifer, der Botmaster (auch Botnetz-Operator oder Bot-Herder genannt), installiert die Bot-Software über eine beliebige Schwachstelle auf den infizierten Maschinen.

Typischerweise kommunizieren Botmaster über einen so genannten Command & Control Server (C&C) mit den kompromittierten Maschinen. Die Bots verbinden sich mit dem C&C-Server, über den sie die Kommandos des Angreifers empfangen. Bei den ersten Generationen von Botnetzen verlief die Kommunikation über das Internet Relay Chat Protokoll (IRC), heute ist das noch bei 40-50 Prozent der Fall. Immer beliebter bei Botmastern wird die Kommunikation über HTTP ohne persistente Verbindung zum C&C-Server. Denn diese erfolgt in Intervallen und ist weniger auffällig als die Interaktion per IRC.

Peer-to-Peer-Botnetze dagegen bestehen aus vielen Servern, meistens aus den Opfermaschinen selbst. Beispiel für ein P2P-Botnetz ist das Spam-Botnet Waledac, welches täglich bis zu 1,5 Milliarden Spam-Mails verschickte und Ende Februar durch einen Gegenangriff von Microsoft und Partnern vom Netz genommen wurde. Waledac funktionierte mit einer teilweise dezentralisierten Kommunikationsstruktur, die aus wenigstens vier Ebenen bestand. Werden Rechner in einem P2P-Botnetz kompromittiert, erhalten diese eine Peer-Liste mit weiteren infizierten Maschinen. Bots erkennen, welche weiteren Maschinen online sind und tauschen Befehle untereinander aus, die der Angreifer zuvor an eine beliebige infizierte Maschine aussendet. Dies erschwert vor allem das Abschalten solcher Botnetze.

Wie Bots Schaden anrichten

Dienten Bots früher noch nur einem Zweck, geht der Trend jetzt zu multifunktionalen Bots, bei denen der Botmaster zwischen verschiedenen Einsatzmöglichkeiten wechseln kann. Bei externen Angriffen wird die Opfermaschine größtenteils dazu missbraucht, Spam- oder Phishing-Mails zu versenden, eigentliche

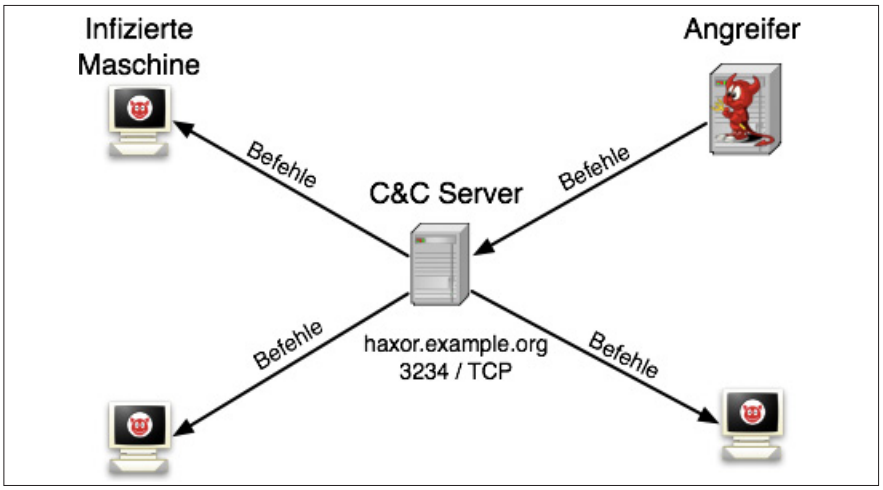


Bild 1: Über den zentralen C&C-Server kontrolliert der Angreifer die Opfermaschinen.

Ursprungsadressen zu verbergen oder Systeme Dritter anzugreifen.

Durch Einsatz eines Proxys wird die Opfermaschine als Zwischenhost genutzt, um nach außen zum Beispiel als Absender von Angriffen oder Webseiten mit illegalen Inhalten zu erscheinen. Ein großes Anwendungsgebiet sind Distributed Denial of Service(DDoS)-Angriffe, bei denen die Zombie-PCs immer wieder die gleiche Anfrage an ein Angriffsziel senden. Die Zielmaschine bricht irgendwann unter der Flut von Kontaktanfragen zusammen und ist nicht mehr erreichbar. Viele bekannte Internetdienste sind bereits Opfer solcher Attacken geworden oder wurden unter Drohung eines Angriffs erpresst.

Für Unternehmen außerhalb der IT-Branche stellen interne Angriffe eine meist größere Bedrohung dar, denn diese gelten den Unternehmensdaten selbst. Lokal gespeicherte Daten werden ausgelesen und zum Angreifer geschickt oder der Netzwerkverkehr abgefangen und nach interessanten Informationen durchsucht. Dies sind die gängigsten Angriffsmuster, doch die Einsatzmöglichkeiten wachsen mit der Phantasie der Angreifer.

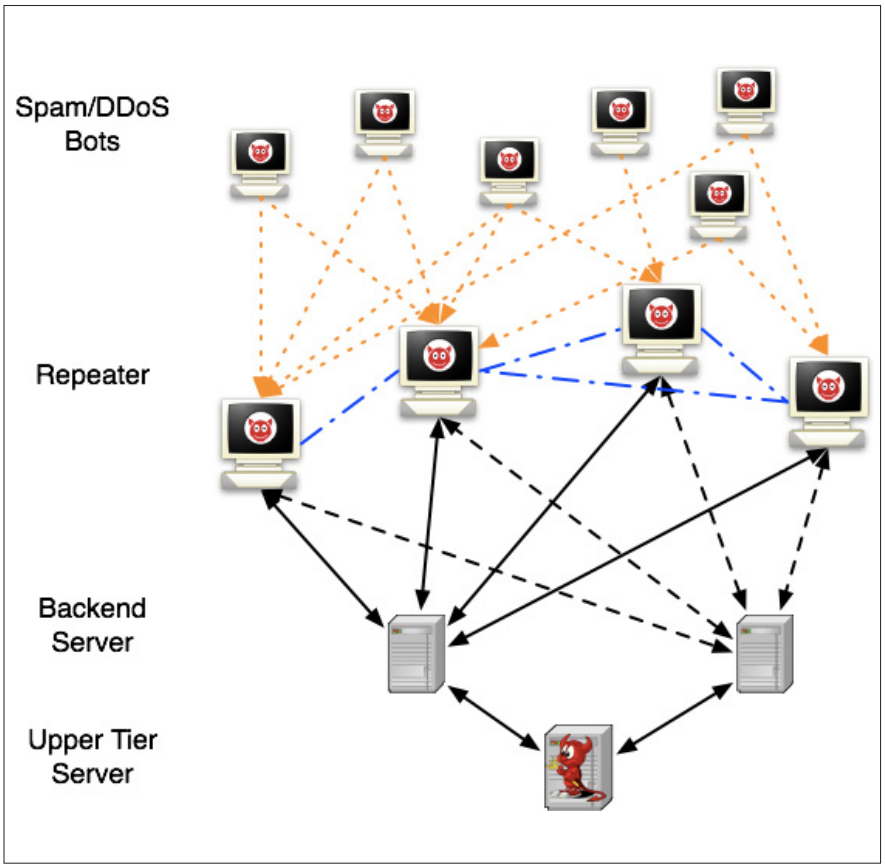


Bild 2: Der Aufbau des Botnetzes Waledac verlief nach dem Peer-to-Peer Prinzip mit dezentraler Kommunikationsstruktur.

Viele Einfallstore

Trotz Millionen-Investitionen großer Konzerne in IT-Sicherheit gelingt es Cyber-Kriminellen, Firmennetzwerke mit Hilfe von Bots zu kapern. Ursachen sind Sicherheitslücken und Schwachstellen – in Software, IT-Infrastruktur oder im Verhalten der Mitarbeiter.

Einfallstor Nr.1 sind heutzutage ungepatchte (oder noch unbekannte) Sicherheitslücken in Third-Party-Programmen wie zum Beispiel dem Acrobat Reader, MS Office oder dem Browser. Bei Browsern kann ein reines Surfen auf einer manipulierten Website ausreichen, um das System zu infizieren. Diese so genannten Drive-by-Downloads sind heute die Hauptverbreitungsmethode von Schadsoftware. An zweiter Stelle folgen E-Mail-Attacken mit infizierten PDFs oder Links zu manipulierten Webseiten. Doch auch Hardware kann als Tor ins Unternehmen dienen: Was bis vor rund zehn Jahren vor allem Disketten waren, sind heute mobile Speichermedien wie USB-Sticks, auf denen sich der Bot via Autorun-Funktion verbreitet.

Interne Verbreitung

Haben es Angreifer geschafft, einen Firmenrechner zu infiltrieren, dient dieser als Sprungbrett für weitere Angriffe. Aggressive Bots versuchen automatisch, Maschinen in der Nähe aufzuspüren, anzugreifen und sich auf diese Art zu verbreiten. Der Nachteil für den Angreifer: Durch die Menge der kompromittierten Maschinen werden Auffälligkeiten sichtbar und der

Bot schnell erkannt. Prominentestes Beispiel hierfür ist Conficker, der sich gerade in Unternehmen aufgrund fehlender interner Schutzmechanismen rasant ausbreitete.

Möchte der Angreifer gezielt in eine Firma eindringen, zum Beispiel zur Industriespionage, fährt er eine andere Weiterverbreitungsstrategie. Er möchte unbemerkt bleiben und infiziert vorerst nur eine oder wenige Maschinen. Der Angreifer loggt sich ein und sucht manuell nach weiteren Maschinen. So geschehen Ende vergangenen Jahres bei der Operation Aurora: Kriminelle nutzten eine bis dato unbekannte Sicherheitslücke im Internet Explorer, um rund 30 Firmen anzugreifen, darunter Google und Adobe Systems. Nach neuesten Berichten könnten sogar über 100 Unternehmen betroffen sein, doch ist noch unklar, ob es sich dabei um die gleichen Hintermänner handelt.

Erkennung von Botnetzen

Hostbasierte Erkennungssysteme setzen auf der Computerebene an: Anti-Viren-Scanner, Spyware oder hostbasierte Intrusion Detection Systeme, die den Datenfluss im IT-System überwachen. Doch befinden sich Antiviren-Industrie und Cyber-Kriminelle in einem Arms Race. In dem Wettlauf scheinen die Angreifer derzeit die Nase von haben, da sie automatisiert neue Versionen ihrer Schadsoftware erstellen können: Hat ein Security-Anbieter eine Signatur für einen neuen Schädling bereit gestellt, kann sich die Signatur in der Zwischenzeit wieder geändert haben. Tests mit Anti-Viren-Software zeigen, dass teilweise nur 40-80 Prozent der Schadsoftware überhaupt erkannt wird. Der hostbasierter Ansatz garantiert kein Aufspüren des Bots und kann nur als Basisschutz verstanden werden.

Weitreichende Analysemöglichkeiten bieten netzwerkbasierte Systeme. Netzwerkbasierte Intrusion Detection Systeme (IDS) zeichnen den Datenfluss im Netzwerk auf und analysieren ihn auf Anomalien. Sie gleichen Signaturen im Netzwerkverkehr mit Signaturen aus Musterdatenbanken ab. Finden IDS eine Übereinstimmung, schlagen sie Alarm. Netzwerkbasierte Intrusion Prevention Systeme (IPS) greifen zusätzlich aktiv in den Datenverkehr ein. Sie verfügen über Module, die Firewall-Konfigurationen beeinflussen und somit indirekt Datenströme stören, unterbrechen oder verändern können.

Entfernung von Bots

Mit herkömmlichen Removal Tools ist es zwar technisch möglich, Bots automatisch zu entfernen, oft können aber nicht alle Spuren und Systemänderungen beseitigt werden. Wirkungsvoller ist eine Kombination aus Anti-Viren-Software und Spyware-Schutz, die nach Start über ein sicheres System wie Linux oder eine Bootsektor-CD zum Einsatz kommen und durch externe Hardware-Firewall sowie softwarebasierte Firewall auf Client-Seite abgeschirmt werden.

Bots erlauben es dem Angreifer oft, weitere schädliche Programme zu installieren. Darum sollte das komplette System auch nach Entfernung des Bots weiterhin unter Beobachtung stehen und auf Anomalien getestet werden. Da Bots Keylogger- oder Sniffer-Funktionen beinhalten können, die zuvor Authentifizierungsdaten ausgespäht haben, sollten sämtliche Passwörter geändert werden. Die sicherste – wenn auch aufwendigste – Variante ist die Neuinstallation des Systems und das entsprechende Rückspielen aller Daten. Voraussetzung ist eine entsprechende IT-Infrastruktur.

Der IT-Administrator

Ein wirkungsvolles Security-Management muss die Angriffsfläche minimieren und technische Hürden für die Angreifer schaffen. Dies beinhaltet kontinuierlich laufende Anti-Viren-Programme, eine externe Firewall, ein Patch-Management für Betriebssystem sowie Software und eventuell netzwerkbasierte Lösungen, die zwar wirkungsvoll, aber auch kostspielig sind. Auch mobile Endgeräte wie etwa Smartphones müssen in diesem Konzept berücksichtigt werden. Bei der Schaffung technischer Hürden muss das Unternehmen zwischen Security und Usability abwägen: Eine automatisierte Sperrung des Internetzugangs beispielsweise mag wirkungsvoll sein, schränkt aber die Mitarbeiter ein.

Hier setzt Security Awareness an: Die Mitarbeiter werden über Datenschutz, IT-Technik und die bestehenden Gefahren aufgeklärt. Ziel: ein gesundes Misstrauen gegenüber fremden E-Mails, Dokumenten und Websites sowie Akzeptanz der bestehenden Security Policy. Die Maßnahmen können isolierte Einzelaktionen beinhalten wie sichere Passwörter, die regelmäßig geändert werden, bis hin zu Testangriffen, die Schwachstellen des Firmennetzes identifizieren. Das größte Sicherheitspotential liegt allerdings in einem ganzheitlichen Schulungskonzept mit konsequenter Umsetzung.

Ausblick

Botnetze sind momentan eines der Hauptprobleme im Internet und es gibt ein breites Spektrum an Angreifern. Auf der einen Seite gibt es minderjährige Cracker, die „aus Spaß" möglichst viele Maschinen kompromittieren und Server lahmlegen möchten. Am anderen Ende der Skala findet sich eine Tendenz zur Professionalisierung. Mit immer subtileren und ausgereifteren Methoden nutzen Angreifer Botnetze zur Industriespionage oder um an vertrauliche Regierungsdaten zu gelangen. Als Land der Hidden Champions hat auch Deutschland Patente, Know-How sowie sensible Unternehmensdaten zu bieten, die hoch im Kurs stehen – vor allem bei Cyber-Kriminellen.

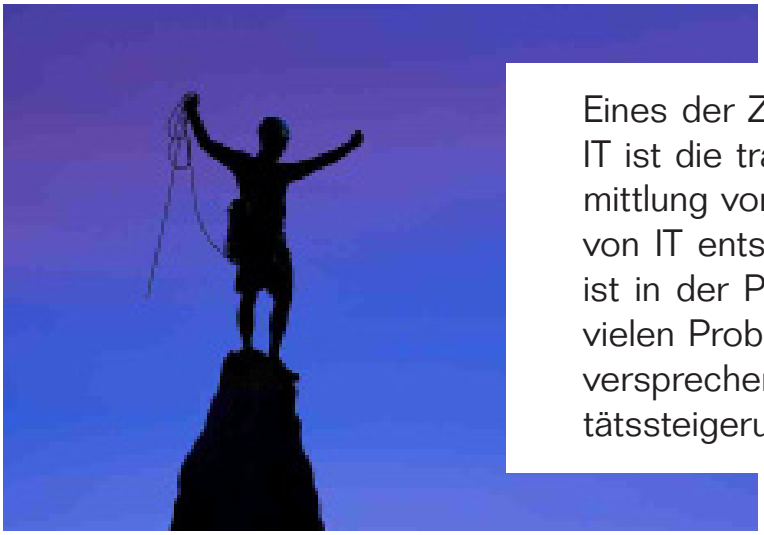
Prof. Dr. Thorsten Holz

„Mit herkömmlichen Removal Tools ist es zwar technisch möglich, Bots automatisch zu entfernen, oft können aber nicht alle Spuren und Systemänderungen beseitigt werden."

Prof. Dr. Thorsten Holz

Prof. Thorsten Holz ist IEEE Member und IEEE-Experte für IT-Sicherheit. Er ist Junior-Professor an der Ruhr-Universität Bochum für „Embedded Systems".

Einsatz von IT-GRC-Plattformen am Beispiel IT-Risikomanagement



Eines der Ziele des Risikomanagements in der IT ist die transparente und nachvollziehbare Ermittlung von Risiken, welche durch den Einsatz von IT entstehen. Die Umsetzung dieses Ziels ist in der Praxis oft ein steiniger Weg und mit vielen Problemen behaftet. IT-GRC-Werkzeuge versprechen hier eine Vereinfachung und Qualitätssteigerung.

In vielen Unternehmen wird immer noch ohne eine vorherige und strukturierte Ermittlung der vorhandenen Bedrohungen über Gegenmaßnahmen entschieden. Leider bleibt bei dieser „bauchgetriebenen“ Vorgehensweise in der Regel unklar, ob die Maßnahmen wirklich ausreichend sind, dem Risiko also angemessen entgegenwirken. Umgekehrt ist unklar, ob der Umfang der ergriffenen Maßnahmen tatsächlich notwendig ist und somit möglicherweise an der falschen Stelle (zu viel) Geld ausgegeben wurde.

Eines der Ziele des Risikomanagements in der IT ist die transparente und nachvollziehbare Ermittlung von Risiken, welche durch den Einsatz von IT entstehen. Nur so kann dem Management eine solide Entscheidungsgrundlage geliefert werden, ob ein Risiko akzeptiert werden kann oder ob entsprechende Gegenmaßnahmen ergriffen werden müssen und wie die Umsetzung dieser Maßnahmen zu priorisieren ist. In diesem Ziel ist man sich in der Praxis überall einig, nur die Umsetzung ist oft ein steiniger Weg und mit vielen Problemen behaftet. IT-GRC-Werkzeuge versprechen hier eine Vereinfachung und Qualitätssteigerung.

Zwei Hauptprobleme

Bei einer näheren Betrachtung des IT-Risikomanagementprozesses in größeren Unternehmen sind häufig zwei Hauptprobleme festzustellen: Kaum jemand hat einen Überblick, welche Risiken derzeit am kritischsten für den eigenen Bereich sind, welche Restrisiken nach der Einführung von Maßnahmen übrig bleiben und wer diese Restrisiken akzeptiert hat und damit die Verantwortung dafür übernommen hat. Es fehlt also an Transparenz und Nachvollziehbarkeit. Darüber hinaus ist die Erfassung der benötigten Informationen wie das Sammeln von möglichen Bedrohungen, Schadenshöhen oder auch nur von etablierten Maßnahmen oft sehr zeitaufwendig und ineffizient.

Eine Ursache hierfür ist unbestritten die hohe Komplexität moderner IT-Landschaften. Viele weitere Ursachen sind jedoch „hausgemacht“, beispielsweise arbeiten die verschiedenen Bereiche oder Abteilungen im Unternehmen, die Risiken betrachten, meist völlig unabhängig voneinander. Dies führt dann dazu, dass diese Bereiche - etwa IT-Sicherheit, Revision, Internal Audit oder die Fachabteilungen - eigenständig Daten erfassen, mit eigenen Methoden Überprüfungen durchführen bzw. Risiken ermitteln, dafür eigene Werkzeuge verwenden und anschließend jeweils individuell aufgebaute Berichte erstellen. Neben einer mangelnden Vergleichbarkeit der

Ergebnisse ist diese Vorgehensweise auch sehr ineffizient, da häufig dieselben Objekte (etwa Applikationen) betrachtet werden, sodass die zuständigen Personen (beispielsweise Applikationsverantwortliche) mehrfach befragt werden und ein redundanter Datenbestand aufgebaut wird.

Ein weiteres verbreitetes großes Problem bei der Durchführung von Risikoanalysen ist die Verwendung hierfür völlig ungeeigneter Werkzeuge, etwa Excel. Solche Tools unterstützen beispielsweise keine Workflow-gestützte Vorgehensweise mit mehreren beteiligten Gruppen und individuellen Sichten auf die Daten (von einer granularen Vergabe von Berechtigungen oder einer Nachvollziehbarkeit von Änderungen ganz zu schweigen) und führen zu einer Unmenge von Dateien auf dem File-Server des jeweiligen Bereichs, die, wenn überhaupt, nur sehr schwer übergreifend ausgewertet können.

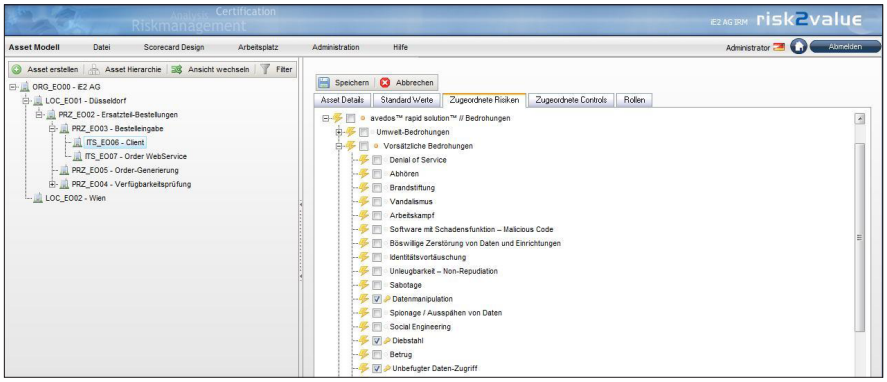


Bild 1: Auswahl von Bedrohungen. Hier und in den nachfolgenden Screenshots dargestellt am Beispiel risk2value von Avedos.

Problematisch ist auch die häufig anzutreffende fehlende ganzheitliche Betrachtung bei Risikoanalysen. Für einzelne Objekte finden zwar Risikobetrachtungen statt, jedoch endet die Betrachtung entsprechend der Zuständigkeit der Abteilung. Beispielsweise betrachtet der IT-Betrieb nur die technische Systemebene, aber nicht die Auswirkungen der erkannten Risiken auf die auf dem System betriebenen Applikationen. Die Fachabteilung wiederum betrachtet zwar die Applikationen, bezieht aber nicht die Ergebnisse der Analysen des IT-Betriebs ein und betrachtet außerdem nicht die Auswirkungen „ihrer" Risiken auf die Geschäftsprozesse, die von den Applikationen abhängig sind.

Viele dieser Probleme können heute mit dem Einsatz so genannter IT-GRC-Werkzeuge gemindert oder gar vollständig beseitigt werden. GRC steht dabei für Governance, Risiko und Compliance. Derartige Werkzeuge haben das Ziel, die verschiedenen Aufgabenbereiche innerhalb der Informationssicherheit zu unterstützen, beispielsweise das IT-Risikomanagement, um dadurch Transparenz und Nachvollziehbarkeit zu schaffen und eine effiziente Durchführung zu ermöglichen.

Anzumerken ist, dass neben der IT sehr viele weitere Anwendungsgebiete für GRC-Werkzeuge existieren. Überall dort, wo im Unternehmen Risiken betrachtet oder Compliance ein Thema ist, kann der Einsatz von GRC-Werkzeugen sinnvoll sein, beispielsweise im Finanz-Risikomanagement oder im unternehmensweiten Risikomanagement. Die beiden großen US-Marktforscher Gartner und Forrester unterscheiden bei GRC zwischen den Marktsegmenten Enterprise GRC und IT-GRC, jedoch sind die Grenzen in der Praxis oft fließend. IT-GRC-Werkzeuge sind speziell auf das Informationssicherheitsmanagement ausgerichtet und verfügen häufig über technische Schnittstellen in die IT. Einige dieser Werkzeuge sind aufgrund ihrer Architektur jedoch so flexibel, dass sie beispielsweise auch im Enterprise Risk Management eingesetzt werden.

Im weiteren Verlauf dieses Artikels wird am Beispiel des IT-Risikomanagements die grundsätzliche Funktionsweise von IT-GRC-Lösungen beschrieben. Viele Produkte bieten jedoch über das Risikomanagement hinausgehende Möglichkeiten, beispielsweise Unterstützung im Compliance-Management oder bei der Verwaltung von Sicherheitspolicies. Bei Letzterem unterstützen die Produkte häufig das Versionsmanagement, die nachvollziehbare Verteilung der Policy an Endbenutzer oder die Verwaltung und Dokumentation von Policy-Ausnahmen.

IT-Risikomanagement mit GRC-Werkzeugen

Bevor das IT-GRC-Werkzeug für die Unterstützung von Risikoanalysen sinnvoll eingesetzt werden kann, müssen die im Rahmen der Risikoanalysen zu betrachtenden Objekte einmalig im System hinterlegt bzw. aus anderen Datenbanken (zum Beispiel CMDB) importiert werden. Je nach Unternehmensorganisation, Aufgabenstellung und Betrachtungstiefe kann es sich bei den Objekttypen zum Beispiel um Gebäude, IT-Systeme, Applikationen, Geschäftsprozesse oder ganze Lokationen handeln.

Die Produkte bieten in der Regel zusätzlich die Möglichkeit, die verschiedenen Objekte hierarchisch miteinander in Beziehung zu setzen. Beispielsweise könnten auf der obersten Betrachtungsebene die Geschäftsprozesse angeordnet werden. Diesen werden dann die sie jeweils unterstützenden Anwendungen untergeordnet und den Anwendungen werden wiederum die IT-Systeme zugeordnet, auf denen die Anwendungen betrieben werden. Auf diese Weise können hierarchische Strukturen bzw. Netzstrukturen geschaffen werden, die es dem Werkzeug später beispielsweise ermöglichen, Risiken von den IT-Systemen zu den Anwendungen und von den Anwendungen bis ganz nach oben zu den Geschäftsprozessen

zu transportieren und so dem Management das Gesamtrisiko transparent zu machen.

Baseline-Ansatz

Die unterschiedlichen Ansätze zur Ermittlung von IT-Risiken, wie sie beispielsweise im TR ISO/IEC 13335-3 beschrieben sind, spiegeln sich auch in den am Markt verfügbaren IT-GRC-Lösungen wieder. So gibt es Produkte, die ausschließlich die so genannte Baseline-Vorgehensweise unterstützen. Die IT-Grundschutzvorgehensweise des BSI ist ein Paradebeispiel für den Baseline-Ansatz. Bei dieser Methodik wird im Rahmen so genannter Control Assessments zunächst der Umsetzungsgrad von Sicherheitsmaßnahmen (Controls) aus einem vorgegebenen Maßnahmenkatalog, der so genannten Baseline, ermittelt.

Die Hersteller von IT-GRC-Lösungen liefern meist fertige Maßnahmenkataloge mit, die sich beispielsweise an den Controls aus den ISO-Standards 27001/27002 oder an den CobiT Control Objectives orientieren. Grundsätzlich ist es aber auch möglich, eigene Kataloge zu hinterlegen, etwa die Maßnahmen der IT-Grundschutzkataloge oder unternehmensspezifische Maßnahmenkataloge, etwa die in einer internen Sicherheitsrichtline enthaltenen Vorgaben oder im technischen Bereich die Maßnahmen aus einer Härtungsanleitung. Nach Auswahl der zu betrachtenden Maßnahmen kann der Umsetzungsgrad bei den meisten Produkten dann entweder in Interviewform über elektronische Fragenkataloge ermittelt oder durch Auswahl eines konkreten Umsetzungsgrads direkt angegeben werden.

Auf der technischen Ebene von IT-Systemen bieten einige Produkte zusätzlich die Möglichkeit, den Umsetzungsgrad der Maßnahmen automatisiert zu ermitteln. Hierzu meldet sich das IT-GRC-Werkzeug mit einem hinterlegten Benutzernamen am Betriebssystem an und fragt für jede Maßnahme des Katalogs über ein jeweils hinterlegtes Skript bestimmte Systemparameter ab (zum Beispiel den

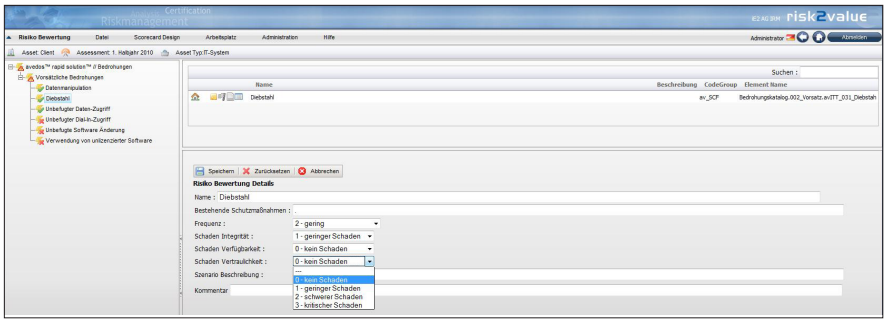


Bild 2: Risikobewertung.

Wert eines Registry Keys). Anhand des Werts ermittelt das Werkzeug dann den Umsetzungsgrad der Maßnahme und berechnet gegebenenfalls einen Risikoindex, welcher ein Maß für den Grad an Nichtumsetzung darstellt.

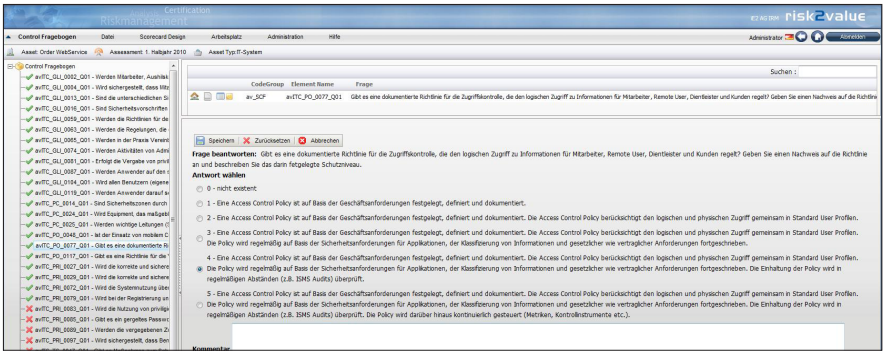


Bild 3: Control Assessment.

Hersteller, die für das Risikomanagement ausschließlich den hier beschriebenen Baseline-Ansatz unterstützen, kommen historisch meist aus dem Compliance-Umfeld. Die Ermittlung des Umsetzungsgrads von Vorgaben bzw. von Maßnahmen ist ja gerade die Kernaufgabe im Compliance-Management und durch die zusätzliche Ermittlung eines Risikoindex wird das Produkt von den Herstellern dann als Risikomanagement-Werkzeug vermarktet.

Detaillierte Risikoanalyse

Andere GRC-Lösungen unterstützen zusätzlich die in deutschen und europäischen Unternehmen verbreitete detaillierte Risikoanalyse in Anlehnung an den Standard ISO/IEC 27005, bei der – stark vereinfacht - zunächst Bedrohungen ermittelt und anschließend bewertet werden.

Produkte, die diesen Ansatz unterstützen, arbeiten grundsätzlich wie folgt: Aus einem im Produkt hinterlegten Bedrohungskatalog werden zunächst die für das betrachtete Objekt relevanten Bedrohungen ausgewählt. Auch hier liefern die Hersteller in der Regel fertige Kataloge mit, beispielsweise basierend auf den im Anhang C des ISO/IEC 27005 enthaltenen Bedrohungen. Selbstverständlich können auch eigene Kataloge entwickelt und hinterlegt werden (Bild 1)

Im nächsten Schritt ermöglicht das GRC-Werkzeug die Bewertung der Bedrohungen, etwa im Hinblick auf den möglichen resultierenden Schaden und die Wahrscheinlichkeit für ein Schadensereignis. Die jeweiligen Werte können dabei vom Anwender wie bei den oben beschriebenen Control Assessments entweder direkt aus einer

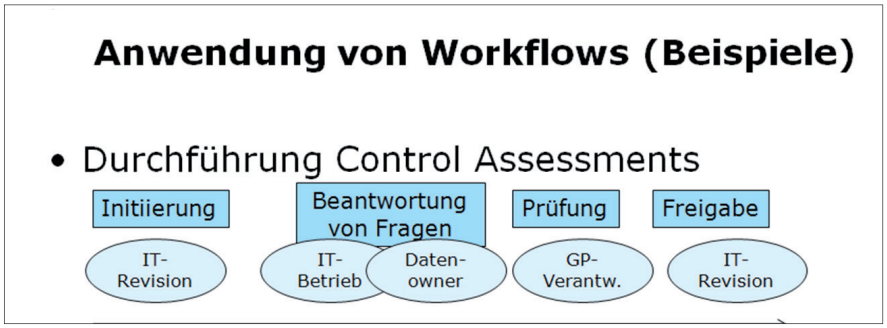


Bild 4: Verknüpfung von Risiken und Maßnahme.

Auswahlliste ausgewählt oder anhand eines Fragenkatalogs in Interviewform ermittelt werden. Anschließend berechnet das Werkzeug über hinterlegte Formeln das zur Bedrohung gehörende Risiko. Viele Produkte geben hier eine starre, nicht durch den Anwender anpassbare Berechnungsmethodik vor (zum Beispiel Produkt von Eintrittswahrscheinlichkeit und Schaden), andere wiederum sind aufgrund ihrer Architektur so flexibel, dass beliebige Formeln hinterlegt werden können und somit die Abbildbarkeit der im Unternehmen eingesetzten Methodik zur Risikoermittlung sichergestellt ist (Bild 2).

Sind die Risiken bekannt, erfolgt im nächsten Schritt die werkzeuggestützte Ermittlung des Umsetzungsgrads von Gegenmaßnahmen (Bild 3). Die Auswahl der zum Risiko „passenden“ Maßnahmen kann dabei ebenfalls durch das Werkzeug unterstützt werden, da in vielen Produkten die Bedrohungen des Bedrohungskatalogs mit den Maßnahmen des Maßnahmenkatalogs verknüpft werden können. Somit kann das Werkzeug für jedes relevante Risiko einen Maßnahmenvorschlag präsentieren. Anhand des Umsetzungsgrads kann das Werkzeug im Anschluss dann das tatsächlich vorhandene (Rest-)Risiko berechnen (Bild 4).

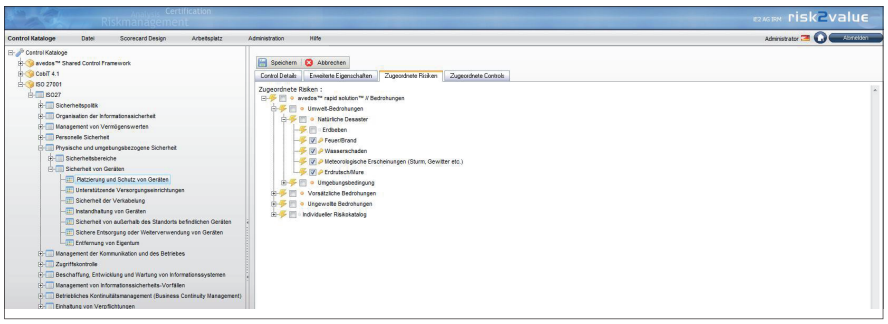


Bild 5: Workflow-Unterstützung in GRC-Werkzeugen.

Sämtliche Arbeitsschritte einer Risikoanalyse werden durch das Werkzeug in ihrer Reihenfolge gesteuert. Durch die Möglichkeit zur Abbildung von Workflows können unterschiedliche Aufgaben an unterschiedliche Rollen bzw. Personen zur Umsetzung delegiert werden. Beispielsweise könnte die IT-Revision mit dem Werkzeug ein Control Assessment initiieren und die sie interessierenden Maßnahmen auswählen.

Anschließend delegiert die IT-Revision die Beantwortung der Fragen zur Ermittlung des Umsetzungsgrads dieser Maßnahmen an den IT-Betrieb. Die entsprechenden Mitarbeiter würden vom Werkzeug über die anstehende Aufgabe per Email benachrichtigt werden bzw. nach Anmeldung am Werkzeug in ihrem persönlichen Aufgabenbereich die Aufgabe angezeigt bekommen. Nach Beantwortung der Fragen würde das Werkzeug dann automatisch wieder die IT-Revision informieren, welche daraufhin beispielsweise die Antworten prüft (Bild 5). Darüber hinaus sind GRC-Werkzeuge mandantenfähig, sodass unterschiedliche Rollen bzw. Personen mit jeweils individuellen Sichten mit dem Werkzeug arbeiten können. Die Produkte verfügen zudem über ein granulares Berechtigungsmodell zur Steuerung des Zugriffs auf die meist sensitiven Informationen.

Projektmaßnahmen

Sind die (Rest-)Risiken ermittelt worden, muss im nächsten Schritt für jedes Risiko entschieden werden, ob es vom Management getragen wird oder durch geeignete Aktivitäten auf ein akzeptables Maß gemindert werden soll.

GRC-Werkzeuge ermöglichen in dieser Phase beispielsweise die Dokumentation dieser Entscheidung sowie die Verwaltung der beschlossenen Projektmaßnahmen zur Risikominderung. Neben der Dokumentation der Aufgaben unterstützen die Werkzeuge meist auch deren Verteilung an den verantwortlichen Personenkreis, ähnlich eines Ticketing-Systems. Gängige Funktionen sind etwa die Pflege des Erledigungsstatus oder eine automatische Erinnerung vor Fälligkeit der Aufgabe (Bild 6).

Berichte und Auswertungen

Eine wichtige Komponente in GRC-Produkten ist die Auswertung und Aufbereitung der durchgeführten Risikoanalysen. Ziel ist es, allen beteiligten Rollen und Personen jederzeit die Ergebnisse im jeweils benötigten Detaillierungsgrad zu liefern. Bei den meisten Herstellern sind einige Standardreports im Lieferumfang enthalten, die jedoch typischerweise noch an das jeweilige Einsatzfeld angepasst werden müssen bzw. komplett neu entwickelt werden. Einige Hersteller bieten darüber hinaus Schnittstellen für den direkten Zugriff auf die Datenbasis, sodass be-

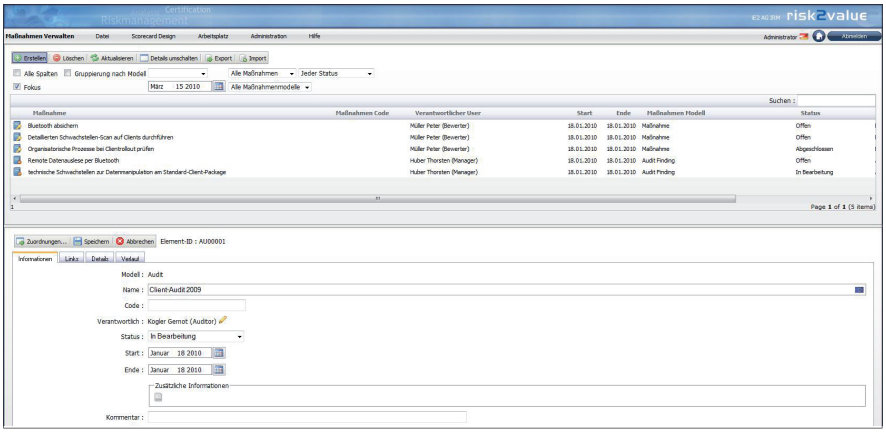


Bild 6: Verwaltung von Projektmaßnahme.

liebige Auswertungen durchgeführt und Reports erstellt werden können.

Die eingangs beschriebene Möglichkeit, verschiedene Objekte hierarchisch miteinander in Beziehung zu setzen, ermöglicht darüber hinaus übergreifende Auswertungen. Beispielsweise können die in den einzelnen Risikoanalysen erkannten Risiken vom Werkzeug entlang der Hierarchie zu einem Gesamtrisiko zusammengefasst werden. Auf dieser Basis könnte das Werkzeug dann jederzeit einen aussagekräftigen Management-Report über die aktuelle Risikosituation erstellen und verteilen (Bild 7).

Risk by Control	Spaltenbeschriftungen			
	Demo Prozesse			Demo Prozesse Ergebnis
Zeilenbeschriftungen	ATLAS LCC	TBD07	TBD08	
IRM Control Catalog	66	43	45	154
Data classification and labeling	5	3		8
Authentication	5	3	3	11
Encryption of data storage	5	3		8
Encryption of NetFlows	5	3		8
Protection from Malware (Virus, Worms, Trojan Code)	5	3	5	13
Authorization	5	3	3	11
Business Continuity and Redundancy	4	5	5	14
Backup of information	4	5	3	12
Operational security	5	5	3	13
Logging	5	3	5	13
Logging of administrator activities	5	3	3	11
Security of system services	5	3	5	13
Application infrastructure	4	1	5	10
Security in software development	4		5	9

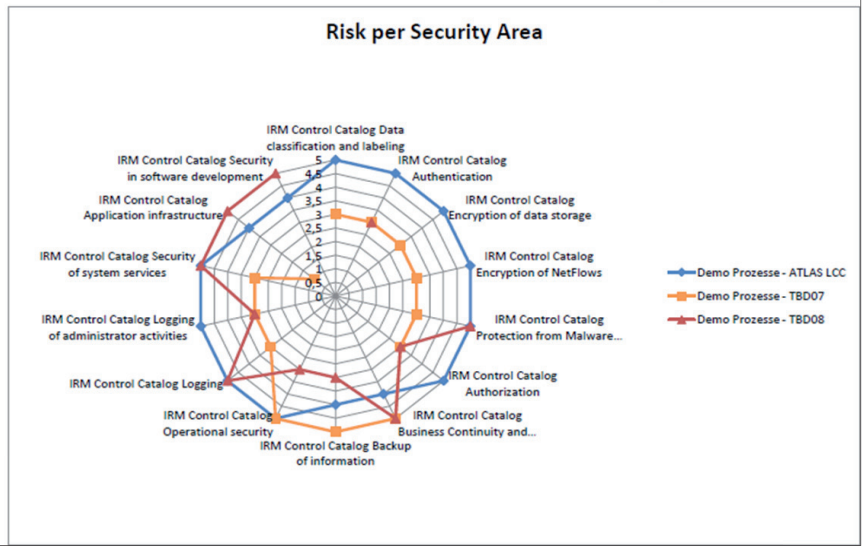


Bild 7: Beispielhafter Report.

Fazit

Heutige IT-GRC-Lösungen bieten ein großes Potential zur Erhöhung der Nachvollziehbarkeit, Transparenz und Effizienz im Informationssicherheitsmanagement. Alle Risiken sind nunmehr an zentraler Stelle nachvollziehbar dokumentiert und dem Management wird die Grundlage gegeben, sich jederzeit einen aktuellen Statusüberblick über die Risikosituation oder die vereinbarten Maßnahmen zu verschaffen und Aktivitäten sinnvoll zu priorisieren

Um diesen Mehrwert tatsächlich zu erzielen, ist eine sorgfältige Produktauswahl erforderlich. Die Produkte unterscheiden sich in ihrem Funktionsumfang und „Reifegrad" teils erheblich. Ein weiterer entscheidender Unterschied zwischen den Produkten ist die Anpassbarkeit an die eigene Methodik und Vorgehensweise. Während viele Produkte feste Formeln zur Risikobewertung vorgeben oder beispielsweise keine Erweiterung der drei Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität zulassen, können in anderen Produkten beliebige Formeln und Berechnungslogiken hinterlegt werden. Die Praxis zeigt, dass am Ende des Auswahlprozesses fast immer eines der zuletzt genannten flexiblen Produkte zum Einsatz kommt - schließlich soll sich das Werkzeug an die Vorgehensweise des Unternehmens anpassen und nicht umgekehrt.

Steffen Gundel

Steffen Gundel, Berater, cirocsec GmbH

SERVICE-ORIENTIERTES

BUSINESS 2010

23.-24. November 2010 in München

Change

von Business/IT-Alignment

Die Industrialisierung der Softwareproduktion

itevents
itverlag

www.sob2010.de

Zurück in die Zukunft

Next Generation Firewalling

In der IT-Sicherheit hat eine Veränderung von Bedrohungen und Angriffen stattgefunden: 16 der SANS Top 20 Threats (www.sans.org) finden auf Anwendungsebene statt.

Auch im öffentlichen Bereich sind Sicherheitsvorfälle durch Einsatz von Peer-To-Peer-Technologien und -Anwendungen zu finden – nicht nur im industriellen Umfeld. Die Entwickler der Technologien um Angriffe erfolgreich durchführen zu können, kennen mögliche Lücken durch klassische Sicherheitsansätze im Firewalling-Umfeld: Kontrolle auf Port-Ebene wie 80 oder 443 ohne in der Lage zu sein, die web-basierte Anwendung zu identifizieren und schon gar nicht zu kontrollieren und vor allem keine SSL-Verbindungen terminieren und damit inspizieren zu können.

Bekannt ist auch dass viele Unternehmen separate Sicherheitsansätze einsetzen wie alleinstehendes IDS/IPS als auch rein inhaltsbasiertes Anti-Virus-Scanning, da sich andere Ansätze auf Grund von zu großen Performance-Einbußen und False-Positive-Vorkommen nicht bewährt haben. Die fehlende Konsolidierung von unterschiedlichen Ansätzen lässt kombinierte Ansätze nicht erkennen. Unified Threat Management (UTM)-Ansätze haben diesbezüglich versagt. Dies nutzt man aus und Firmen sind nicht in der Lage, die Nutzung von Anwendungen im öffentlichen Internet zu kontrollieren.

Zudem werden Benutzer in Unternehmen zunehmends kreativer. Während niemandem etwas Böses

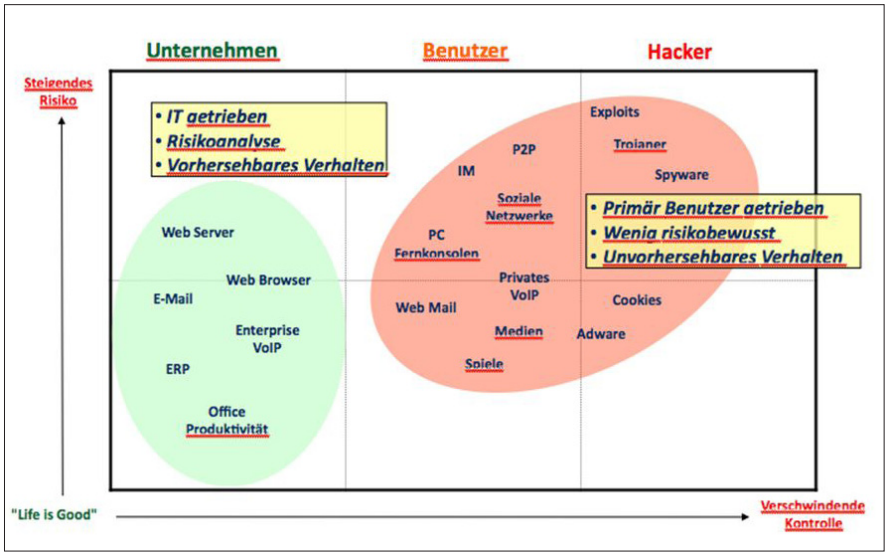


Bild 1: Das Risiko angegriffen zu werden, steigt im privaten Umfeld.

zu unterstellen ist, wenn im Büro die gleichen Ressourcen wie im privaten Bereich durch vorsätzliches Umgehen gezielten bösartigen Angriffe auf unternehmerische Ressourcen und Werte, um an vertrauliche Informationen

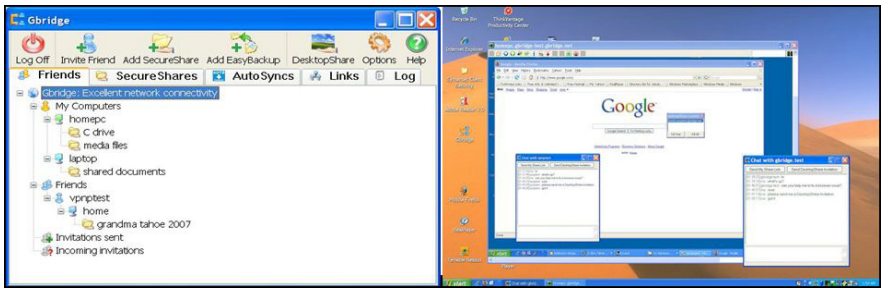


Bild 2: Gefahrenquelle Internet.

beispielsweise von URL-Kategorisierungen genutzt werden – privates und berufliches Leben werden zunehmend miteinander vermischt – gibt es die zu gelangen oder einem Unternehmen zu schaden. Beides, das Kommunikationsverhalten des kreativen Endanwenders im Unternehmen als auch die

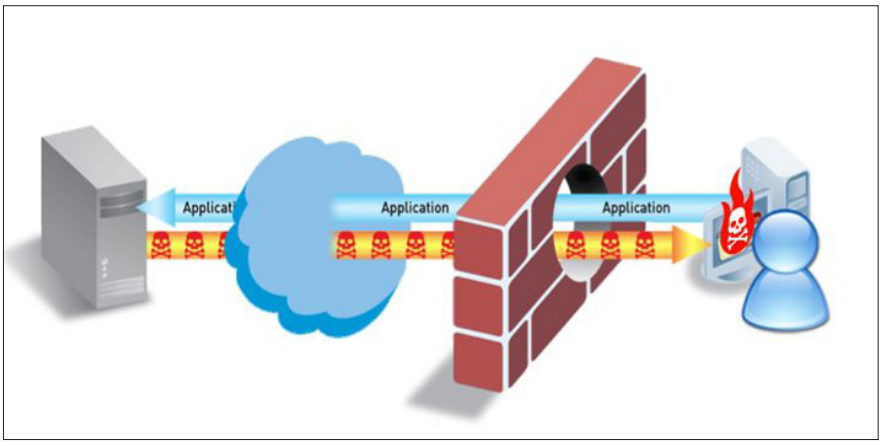


Bild 3: Gefahren sind latent immer vorhanden.

gezielten, kombinierten und ständig wechselnden Angriffe auf Unternehmenswerte sind nur schwer, wenn überhaupt vorherzusehen oder zu erahnen (Bild 1).

Während der Unternehmensmitarbeiter Web-Browser-basierte Anwendungen nutzt um auf Ressourcen im öffentlichen Internet zuzugreifen um in beide Richtungen Inhalte zu übertragen wie er es im privaten Leben von zu Hause gewohnt ist, versucht der Angreifer die Kontrolle über Unternehmensressourcen zu gewinnen in dem er aktive Funktionen auf Arbeitsplätzen installiert oder Endanwender auf nicht erkennbare Funktionen im Internet ansetzt. Beide Vorgänge sind für klassische Technologien wie sie weitegehend seit Jahren eingesetzt werden nicht zu erkennen. Um diesem entgegenzutreten gilt es im ersten Fall – Endbenutzer - Anwendungsfunktionen zu erkennen und im zweiten Fall – Angreifer – Angriffsvektoren auch kombinierter Angriffe darzustellen.

Auch wenn dies nicht einfach ist, rechtfertigt dies keineswegs eine Kapitulation oder Akzeptanz bis hin zu Schulterzucken. Sogenanntes Port-Hopping wird lange nicht mehr nur von dem allseits bekannten Skype eingesetzt. Ist dieses nicht erfolgreich wechseln auch andere ‹Plattformen› sehr schnell auf das nur schwer wenn überhaupt auf Anwendungsfunktionen kontrollierbare Protokoll HTTP (Port 80), noch schlimmer einschließlich Verschlüsselung durch den Einsatz von SSL-Tunneln (Port 443) die Unternehmen heute nur sehr selten aus nicht-technischen Gründen terminieren und entschlüsseln dürfen. Um nur von den meist missbrauchten Protokollen zu sprechen und vorerst noch gar nicht etwa über das Protokoll DNS – welches sich technisch hervorragend zum Tunneln eignet – zu erwähnen.

Hier nur ein Beispiel, das sich ohne technische Kenntnis alle möglichen Inhalte wie Dateien auf dem eigenen Computer im Unternehmen über einen verschlüsselten Tunnel (OpenVPN) einem gegenüber im Internet zur Verfügung zu stellen oder über den gleichen, verschlüsselten Weg einen entfernten PC über das öffent-

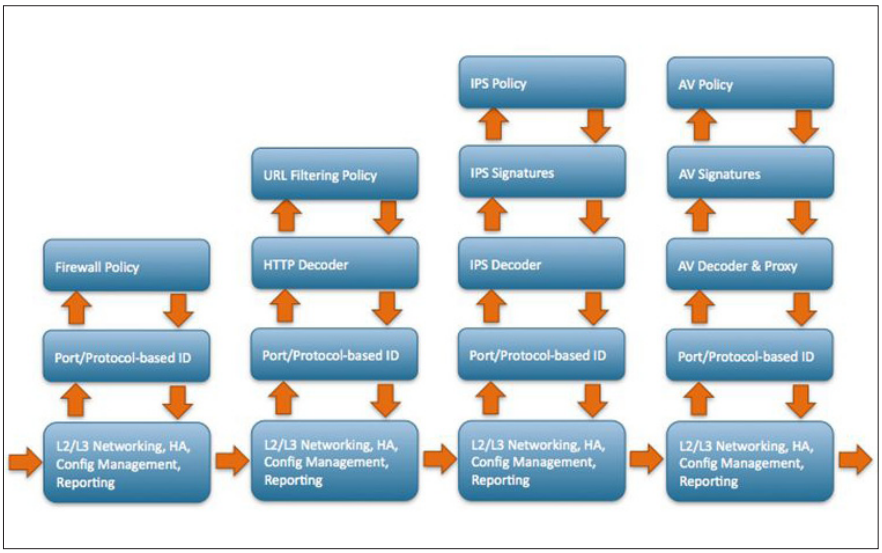


Bild 4: Der klassische Unified Threat Management-Ansatz hat ausgedient.

liche Internet fernzubedienen, wenn sich der Vorgang nicht erkennen lässt, bevor der Tunnel hergestellt werden kann (Bild 2).

mer noch nur Viren und Trojaner gesehen. Dies sind heute jedoch nur die Technologien, die eingesetzt werden, um den eigentlichen Angriff zu starten: den Zugriff auf firmeninterne Ressourcen und das Übertragen von internen Informationen an nicht berechtigte Interessenten. Letztendlich

IT-Verantwortliche von Netzwerkinfrastrukturen haben mit der Weiterentwicklung von Anwendungen und der Nutzung des öffentlichen Internets die Visualisierung und Kontrolle ihrer IT-Ressourcen verloren und müssen diese wieder zurück gewinnen. Und dieses Ziel ist nicht mit den herkömmlichen Methoden der letzten 10 Jahre – und letztlich ist damit die klassische Firewall-Technologie von vor 10 Jahren gemeint – zu erreichen.

Über den Sicherheitsaspekt hinaus, ist natürlich der Faktor der Aufwände eine IT-Infrastruktur den organisatorischen Herausforderungen und Reibungsverlusten entsprechend zu betreiben nicht zu vergessen. Dieses lässt sich nur durch einen neuen Ansatz und dafür von Grund auf entwickelte Lösungen zu erreichen: The Next Generation Firewall.

Selbst Gartner unterstreicht dies mit dem jüngst erschienen „Magic Quadranten“ für netzwerkbasierende Unternehmens-Firewalls.

Um Netzwerkkommunikationen bis hin zur Anwendungsfunkti-

File Sharing.

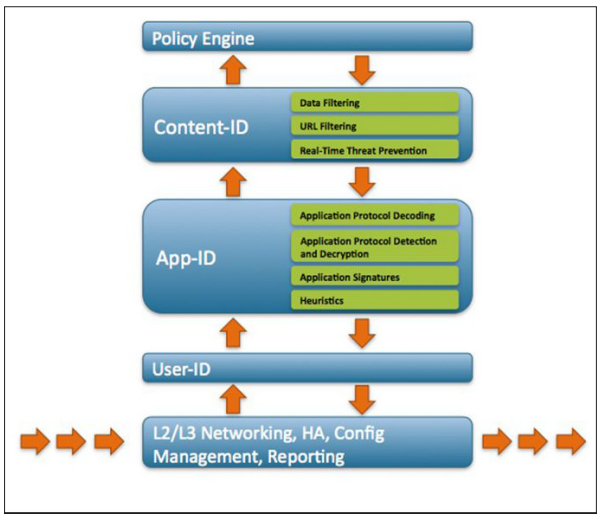


Bild 5: Analyse und Kontrolle sind in einer Prozessabfolge zusammengefasst.

Remote Desktop.

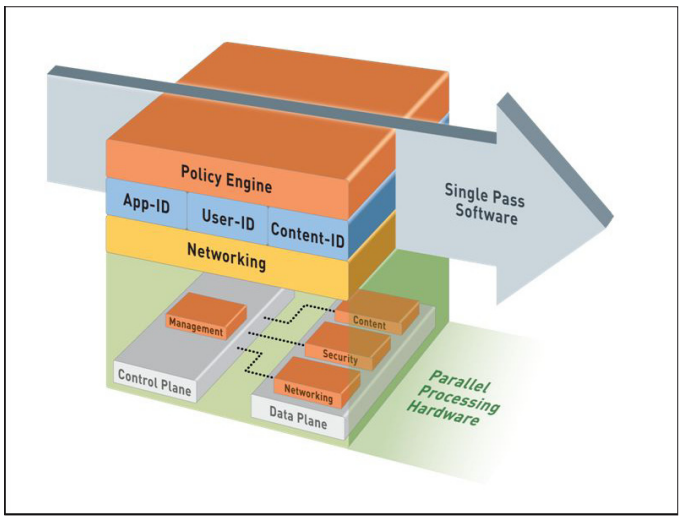


Bild 6: So sieht eine moderne Firewall-Architektur aus.

Ohne Kontrolle ist es möglich, bei Nutzung von Anwendungen im Internet auf dem Rückweg ins Unternehmen diese für Angriffe zu missbrauchen (Bild 3).

Vielerorts werden als Angriffe im-

ist der Prozess der durch einen Virus oder Trojaner möglich ist, nicht anders als das missbräuchliche Benutzen von multifunktionalen Anwendungen, um Informationen zu übertragen.

on darzustellen und zu kontrollieren, sind diese in einem vereinheitlichten und umfassenden Prozess zu analysieren. Dieses ist nicht möglich im klassischen UTM- („Unified Threat Management»)-Ansatz, zu dem es seit

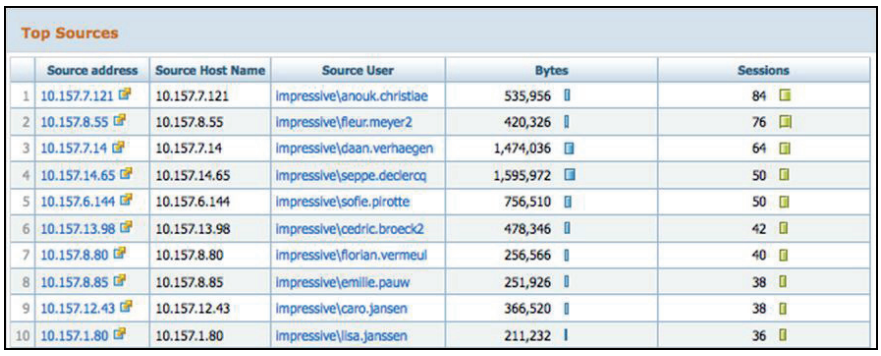
Top Applications

	Risk	Application	Sessions	Bytes
1	4	web-browsing	633	14,177,082
2	2	ping	367	44,040
3	3	teamviewer	96	431,338
4	5	gbridge	76	131,254
5	4	facebook	55	473,682
6	4	dns	46	96,408
7	1	unknown-udp	6	16,602
8	2	google-analytics	5	38,818
9	4	flash	3	167,212
10	4	google-talk	3	175,351
11	3	facebook-chat	2	11,104
12	1	unknown-tcp	2	92,768
13	2	silverlight	1	118,579

Top Applications

	Risk	Application	Sessions	Bytes
1	4	web-browsing	325	48,330,648
2	1	unknown-udp	66	4,560
3	4	facebook	52	333,216
4	4	ssl	48	185,354
5	3	yahoo-mail	28	8,835,568
6	4	flash	20	538,644
7	4	yahoo-im	8	20,760
8	4	dns	6	1,754
9	2	google-analytics	4	14,484
10	4	ms-update	2	5,074
11	1	unknown-tcp	2	47,032
12	2	google-safebrowsing	2	134,074

Bild 7: Detaildarstellung Anwendungen.



Top Sources

	Source address	Source Host Name	Source User	Bytes	Sessions
1	10.157.7.121	10.157.7.121	impressive\anouk.christiae	535,956	84
2	10.157.8.55	10.157.8.55	impressive\fleur.meyer2	420,326	76
3	10.157.7.14	10.157.7.14	impressive\daan.verhaegen	1,474,036	64
4	10.157.14.65	10.157.14.65	impressive\seppe.declercq	1,595,972	50
5	10.157.6.144	10.157.6.144	impressive\sofie.pirotte	756,510	50
6	10.157.13.98	10.157.13.98	impressive\cedric.broeck2	478,346	42
7	10.157.8.80	10.157.8.80	impressive\florian.vermeul	256,566	40
8	10.157.8.85	10.157.8.85	impressive\emilie.pauw	251,926	38
9	10.157.12.43	10.157.12.43	impressive\caro.jansen	366,520	38
10	10.157.1.80	10.157.1.80	impressive\lisa.janssen	211,232	36

Bild 8: Detaildarstellung Benutzer.

	Receive Time	Type	File Name	Name	ID	From Zone	To Zone	Source	Destination	From User	To User
	04/12 03:48:19	file	wsus3setup.cab	Microsoft Cabinet (CAB)	52003	tapzone	tapzone	65.54.75.115	10.157.8.12		impressive\una.goossens
	04/12 03:48:15	file	savcorp10%20oem_microdefsb.jun_symalllanguages_livetri.zip	ZIP	52004	tapzone	tapzone	198.189.255.73	10.157.1.202		impressive\jason.delvaux
	04/12 03:48:15	file	Discussion Blog.doc	Microsoft Word	52012	tapzone	tapzone	10.157.7.14	67.170.203.50	impressive\daan.verhaegen	
	04/12 03:48:15	file	Discussion Blog.doc	Microsoft Word	52001	tapzone	tapzone	10.157.7.14	67.170.203.50	impressive\daan.verhaegen	
	04/12 03:47:55	file	0011 Covering Hard News Pt II.ppt	Microsoft PowerPoint	52011	tapzone	tapzone	10.157.7.14	75.36.220.94	impressive\daan.verhaegen	
	04/12 03:47:55	file	0011 Covering Hard News Pt II.ppt	Microsoft PowerPoint	52000	tapzone	tapzone	10.157.7.14	75.36.220.94	impressive\daan.verhaegen	
	04/12 03:47:52	file	Grammar Quiz 1.doc	Microsoft Word	52001	tapzone	tapzone	10.157.7.14	68.126.188.79	impressive\daan.verhaegen	

Bild 9: Detaildarstellung Inhalt.

Bild 10: Die kritischen Stellen werden visualisiert dargestellt.

Jahren zahlreiche Produkte gibt (Bild 4).

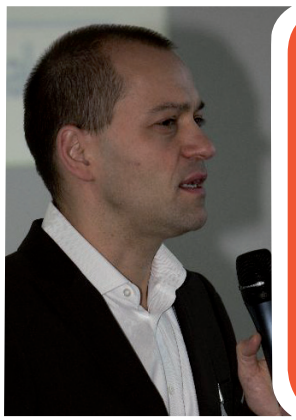
An seine Stelle ist ein umfassender Prozess erforderlich der in einem Schritt die komplette Kommunikation (Anwendungen/App-ID, Benutzer/User-ID, Inhalte/Content-ID) analysiert und diese in einer Regel kontrolliert (Bild 5).

Dieses wird erreicht durch eine speziell dafür entwickelte Soft- (Betriebssystem) und Hardware- (Appliance mit anwendungsspezifischer, programmierbarer Hardware) Plattform (Bild 6).

So ist es möglich, in erforderlicher Leistungsfähigkeit (Gbps Durchsatz, kleiner 1 Millisekunde Laufzeit) die Anwendungskommunikationen umfassend wie detailliert darzustellen was die Information Anwendung, Benutzer und Inhalt mit einschließt Bild 7-9).

Die umfassende bis sehr detaillierte Visualisierung (Bilde 10) ermöglicht die Definition von entsprechenden Sicherheitsrichtlinien zur Anwendung in der Unternehmensfirewall, die nun auch Benutzer (Active Directory, LDAP, RADIUS), Anwendung (Facebook Email & Chat, Webex Office & Desktop Sharing) als auch Inhalte (Viren, Spyware, Vulnerabilities, URL-Kategorie, Dateitypen, Datenpattern) in einer Regel zur Sperrung, Zulassung, Bandbreitenbeschränkung oder -Garantie wie Benutzer- und Anwendungs-abhängiges Routing ermöglicht.

Achim Kraus



„IT-Verantwortliche von Netzwerkinfrastrukturen haben mit der Weiterentwicklung von Anwendungen und der Nutzung des öffentlichen Internets die Visualisierung und Kontrolle ihrer IT-Ressourcen verloren und müssen diese wieder zurück gewinnen."

Achim Kraus

Engineer, Palo Alto Networks