8MAN

Access Rights Management. Only much Smarter.

DIE DREI STOLPERSTEINE DER IT-SICHERHEIT

Protected Networks

IT-SICHERHEIT IM FOKUS

DIE DREI STOLPERSTEINE DER IT-SICHERHEIT UND IHRE ÜBERWINDUNG

Abstract:

Initiativen für mehr IT-Sicherheit sind häufig ineffektiv. Die Gründe dafür lassen sich auf drei Stolpersteine reduzieren: die einseitige Wahrnehmung der Bedrohungslage, die Umsetzung von Initiativen mit dem starren Fokus auf Sicherheit und die Reduzierung von IT-Sicherheit auf eine Unternehmensrolle.

Am Beispiel der Access-Rights-Management-Lösung 8MAN wird deutlich, wie die Umgehung der Stolpersteine 8MAN zu einer breit akzeptierten und praxistauglichen Sicherheitslösung gemacht hat.

1. DIE DREI STOLPERSTEINE DER IT-SICHERHEIT

1.1. Der einseitige Blick auf die Bedrohungslage

Im Bereich der IT-Sicherheit gibt es derzeit Diskussionen um neue Technologien und daraus resultierende Gefahren durch die professionalisierte Hackerindustrie. Beides hängt miteinander zusammen. Mobile Endgeräte, Cloud-Computing und Virtualisierung weichen die Grenzen zwischen IT-Anwendungen und Unternehmensnetzwerken auf. Auch Meldungen von spektakulären Cyberattacken auf prominente Einrichtungen, wie den Deutschen Bundestag oder prominente Medienunternehmen, richten den Fokus der Diskussion auf Gefahren von außen.

IT-Sicherheit vor externen Bedrohungen ist für Unternehmen, Regierungsinstitutionen und Behörden nicht mehr wegzudenken. Trotzdem ist der einseitige Blick nach außen trügerisch. Er ergibt sich aus realistischen Bedrohungen, ist aber auch stark von medienwirksamer Berichterstattung geprägt. Darüber hinaus wirkt ein simpler Mechanismus: Menschen neigen dazu, Sicherheitsprobleme zu externalisieren.

Die Folge: Die Mauern um das Firmennetzwerk werden erhöht und die Abgrenzungen von Bereichen innerhalb des Netzwerkes geraten aus dem Blick. Die „Innentäter", die sich oftmals völlig frei im Unternehmensnetzwerk bewegen, werden ignoriert. Dabei greift eine Vielzahl von Mitarbeitern auf Wissen und Daten zu. Dadurch entstehen Sicherheitsrisiken: Kundendaten, Projekte und Prototypen sind ungesteuert einsehbar und lassen sich unentdeckt kopieren.

> „55 Prozent der Sicherheitsattacken stammen von Datendieben mit Zugriffsrechten."

Die Brisanz: Laut dem IBM Cyber Security Intelligence Index stammen 55 Prozent der Sicherheitsattacken von Datendieben mit Zugriffsrechten. Neben Schutzmechanismen gegen externe Bedrohungen, wie z. B. Firewalls, gehören auch die Kontrolle und gesteuerte Vergabe von Zugriffsrechten zum Einmaleins der IT-Sicherheit.

1.2. Sicherheitsmaßnahmen, die Arbeitsprozesse bremsen

Sicherheitsinitiativen sind meistens gut gemeint, scheitern jedoch an einer zentralen Hürde. Sie richten ihren Blick nur auf die Erhöhung der Sicherheit. Sicherheit ist jedoch für sich alleinstehend zu abstrakt, um für die Endanwender einen erkennbaren Mehrwert zu bieten. IT-Sicherheitsvorfälle, insbesondere innerhalb des Firmennetzwerkes, werden selten erkannt und bleiben dadurch außerhalb der Erfahrungswelt der meisten Mitarbeiter.

Erschwerend kommt hinzu: Interventionen, die nur die Erhöhung der Sicherheit zum Ziel haben, schränken Mitarbeiter in ihren Arbeitsprozessen ein. Die Folge sind Abweichungen von den neuen Richtlinien, mit denen sich die gewünschten Ergebnisse in das Gegenteil verkehren. Im Grunde liegt das Problem darin, dass normalerweise Sicherheit und Effizienz im Widerspruch zueinander stehen.

> „IT-Sicherheitsmaßnahmen müssen gleichzeitig erkennbare Erleichterungen für die Anwender mit sich bringen."

Deshalb bleibt nur die nüchterne Erkenntnis: IT-Sicherheitsmaßnahmen müssen gleichzeitig erkennbare Erleichterungen für die Anwender mit sich bringen. Ist dies nicht der Fall, leidet die Akzeptanz für die Intervention. Deshalb ist es ratsam, den Fokus zu verändern. Nicht die Frage nach mehr Sicherheit sollte als Erstes gestellt werden, sondern wie sich bestehende sicherheitsrelevante Prozesse vereinfachen lassen.

1.3. Die Zentralisierung von Sicherheitskompetenz

Der steigende Bedarf an IT-Sicherheitslösungen hat zahlreiche mehr oder weniger entwickelte Rollen in Unternehmen geschaffen: Datenschützer, Auditoren, IT-Sicherheitsbeauftragte und Information Security Manager entwickeln Initiativen und Kontrollinstrumente, um die Voraussetzungen für mehr IT-Sicherheit und Datenschutz zu schaffen. Damit ist aus Unternehmenssicht ein wichtiger Schritt getan. Dennoch unterliegen nicht wenige dem Trugschluss, die Sicherheitsfrage sei damit vollständig beantwortet. Schlimmer noch: Oft wird mit den Rollen die Sicherheitskompetenz im Unternehmen vollständig zentralisiert und auf die genannten Rollen beschränkt.

Das Problem: Sicherheitskompetenz lässt sich nicht akkumulieren. Sie muss sich zumindest bei den Führungskräften dezentral im Unternehmen entwickeln. Daten ,Informationen und Wissen – was davon schützenswert ist und wer darauf Zugriff haben sollte, kann nur in den Fachabteilungen entschieden werden.

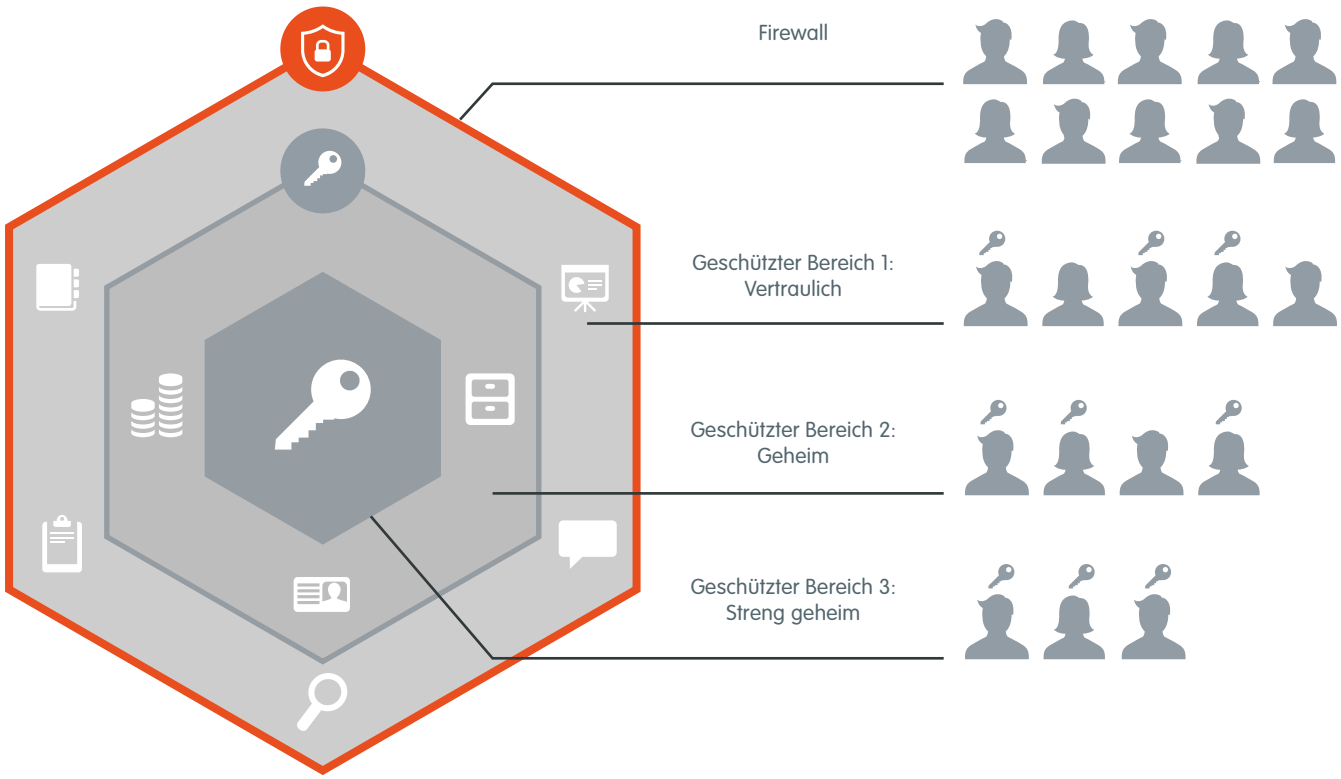
Die Lehre:

Ohne praxisbezogene, für das Handlungsumfeld der Führungskraft maßgeschneiderte Verantwortlichkeiten scheitert jede Sicherheitsinitiative.

2. DAS IT-SICHERHEITSKONZEPT VON 8MAN

Entstanden ist 8MAN aus der Überlegung heraus, den Blick auf IT-Sicherheit nach innen zu richten. Die Firewall stellt die erste Abgrenzung dar.

Doch auch innerhalb eines Netzwerkes muss die Existenz geschützter Bereiche sichergestellt werden. Dies ergibt sich allein schon aus unterschiedlichen Geheimhaltungsstufen für sensibles Wissen. Daten, Informationen und Wissen liegen im Netzwerk in unterschiedlichen Bereichen. IT-Sicherheit beginnt bei der Strukturierung und dem Schutz der Inhalte vor falschem Zugriff.



Die Ausbildung geschützter Bereiche im Firmennetzwerk ist ein Stiefkind der IT-Sicherheit. Der Grund: Selbst für spezialisierte Administratoren ist das Firmennetzwerk schwer von innen zu schützen. Die Analyse, Dokumentation, Überwachung und Veränderung von Zugriffsrechten ist zeitintensiv und stellt die IT vor erhebliche Probleme.

Bei der Verwaltung des Active Directory müssen Administratoren die Gruppenstrukturen im Blick behalten und die Zugriffsrechte ihrer Kollegen auf Fileserver, SharePoint, vSphere und Exchange-Ressourcen gemäß ihrer Rolle gestalten. Die Rechteverwaltung erfolgt in verschiedenen Oberflächen, mit denen die Erfassung der Ist-Berechtigungssituation nicht effizient und zentralisiert möglich ist. Verschachtelte Gruppenstrukturen lassen sich nur unter Konsolidierung mehrerer Quellen aufdecken.

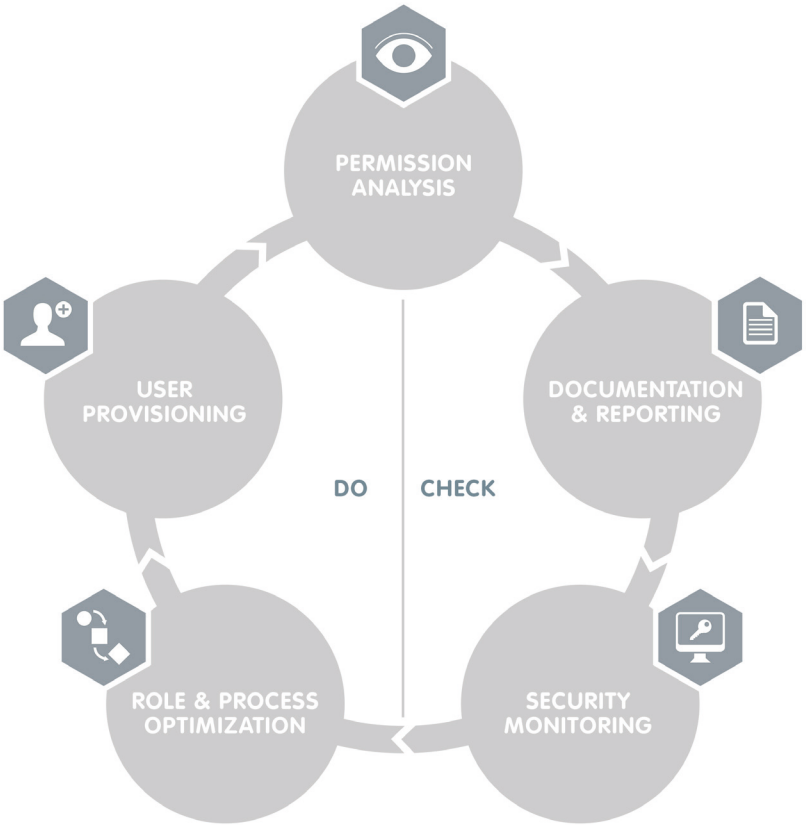
> „Der 8MAN Ansatz setzt problemorientiert an der Vereinfachung sicherheitsrelevanter Prozesse an."

Der 8MAN Ansatz setzt problemorientiert an der Vereinfachung sicherheitsrelevanter Prozesse an. Denn nur so kann ihre Umsetzung garantiert werden. Mit den fünf Basisservices Permission Analysis, Documentation & Reporting, Security Monitoring, Role & Process Optimization und User Provisioning schafft 8MAN die Voraussetzung für die Umsetzung interner IT-Sicherheit.

2.1. Access Rights Management als Basis für IT-Sicherheit

Mit **Permission Analysis** können Administratoren erstmals ressourcenübergreifend die Berechtigungssituation im Firmennetzwerk erfassen. 8MAN zeigt in einer zentralen Ansicht die Gruppenmitgliedschaften aus dem Active Directory und die Zugriffsrechte für Fileserver, SharePoint, Exchange und vSphere. Dieses Wissen ist die Voraussetzung, um Sicherheitslücken zu erkennen und Maßnahmen einzuleiten.

Um Anforderungen der IT-Sicherheit, gesetzlicher Regularien und Auditoren zu erfüllen, verwenden Verantwortliche viel Zeit auf Dokumentation. Der Service **Documentation & Reporting** setzt genau an dieser Hürde an. Mit wenigen Klicks ist die Zugriffsrechtehistorie ersichtlich und sind revisionssichere Reporte erstellt. Diese lassen sich automatisiert an die Geschäftsführung, IT-Leiter, Datenschützer und Auditoren versenden.



Die herkömmliche Analyse von Zugriffsrechten beschränkt sich auf die Erfassung der Ist-Situation von Zugriffsrechten. Mit dem 8MAN **Security Monitoring** lassen sich alle sicherheitsrelevanten Aktivitäten im Firmennetzwerk und auf Fileservern erfassen. Damit wird eine zentrale Sicherheitslücke geschlossen: Selbstvergebene Zugriffsrechte mit dem Ziel des Datendiebstahls bleiben nicht mehr unter dem Radar. Darüber hinaus lassen sich besonders sicherheitsrelevante Verzeichnisse auf dem Fileserver permanent und bis auf Dateiebene überwachen.

Sicherheit geht alle an. Sie ist zu wichtig, um sie zu zentralisieren. Deshalb setzt 8MAN mit **Role & Process Optimization** auf das Data-Owner-Konzept. Data Owner sind Führungskräfte und strukturell gesehen der beste Adressat, wenn es um die Einschätzung und Klassifizierung von schützenswertem Wissen geht. Darüber hinaus sind sie als direkte Schnittstelle zu ihren Mitarbeitern in der Lage zu entscheiden, wer wo Zugriff haben sollte. Mit 8MAN bleibt interne Sicherheit keine Richtlinie auf dem Papier. Es lassen sich für jeden Fachbereich Data Owner nominieren. Diese vergeben in einem einfachen Interface die Zugriffsrechte für ihre Mitarbeiter und können geschützte Verzeichnisse für sensibles Wissen auf dem Fileserver anlegen.

„8MAN dezentralisiert Sicherheit und trägt Security Awareness in das Unternehmen."

8MAN dezentralisiert Sicherheit und trägt mit der Verleihung von Verantwortung an Data Owner Security Awareness in das Unternehmen. Der Administrator ist nicht mehr Teil des Prozesses und kann sich auf seine Projekte konzentrieren.

User Provisioning umfasst die Anlage neuer Nutzerkonten, die Rechteverwaltung und die Bearbeitung von Kontodetails. Alle diese Aufgaben können im 8MAN ohne Medienbruch und durch verschiedene Rollen ausgeführt werden. Standardoperationen, wie z. B. die Useranlage und das Account Management, werden so an den Helpdesk delegierbar.

2.2. Wie Sie Ihr Unternehmen sichern

Die Einführung von 8MAN ist kein Projekt, sondern ein Griff zum Telefon. Vereinbaren Sie einen Termin und ein zertifizierter Techniker wird die Installation und Konfiguration bei Ihnen im Unternehmen vornehmen. Je nach den Möglichkeiten in Ihrem Unternehmen kann die Installation vollständig via Remote Access vorgenommen werden.

Kostenloses Webinar

Starten Sie mit einer 30-minütigen Führung und sehen Sie den 8MAN in Aktion. Als Teilnehmer bleiben Sie untereinander anonym. Sie haben die Möglichkeit, am Ende der Präsentation im Chat Fragen zu stellen.

Kostenlose Teststellung

Testen Sie 8MAN mit einer 21 Tage gültigen kostenlosen Testlizenz und Sie haben genug Zeit, sich von unserer Lösung in Ruhe zu überzeugen.

Kontakt

Adresse:
Protected Networks GmbH,
Alt Moabit 73,
10555 Berlin,
Deutschland

Website:
http://www.8man.com

Telefon:
+49 30 3906345-0

E-Mail:
info@8man.com

Autor:
Fabian Fischer
Knowledge Manager | 8MAN