

Empirum 2008

Empirum Security Suite und IT-Grundschutz nach BSI
von Allar Networks & Consulting GmbH



1. Das Unternehmen	4
2. Über Empirum Security Suite	5
2.1. Einführung	5
2.2. Wie schützt die Empirum Security Suite Ihr Unternehmen?	5
3. Aufgabenstellung / Allgemein	7
3.1. IT-Grundschutz nach BSI	7
4. Betrachtung	7
5. Modellierung	8
5.1. Übergreifende Aspekte	8
5.1.1. Organisatorische Mängel	8
5.1.2. Kryptokonzept	8
5.1.3. Hard- und Software Management	8
5.2. IT-Systeme	9
5.2.1. Clients	9
5.3. Netze	9
5.3.1. Netze allgemein	9
5.3.2. WLAN	9
5.4. Anwendungen	10
5.4.1. Mobile Datenträger	10
6. Zusammenfassung	10



Empirum Security Suite und IT-Grundschutz nach BSI

Analyse zur Umsetzung der Anforderungen von Maßnahmen nach IT-Grundschutz mit Hilfe der Empirum Security Suite



Allar Networks & Consulting GmbH
Engenser Straße 59
56170 Bendorf
<http://www.allar.net>
info@allar.net
Fon: +49.2622.1207-0
Fax: +49.2622.1207-77

ESS und IT-Grundschutz nach BSI

1. Das Unternehmen

Das Unternehmen matrix42 AG konzentriert sich seit über 10 Jahren auf den Bereich Automatisierung und Management von Desktop- und Server-Systemen. Durch den im Markt einzigartigen Ansatz eines integrierten Daten- und Prozess-Managements ist matrix42 AG in der Lage, im Betrieb unterschiedlichster IT-Infrastrukturen hohe Einsparungspotentiale durch größtmögliche Prozessautomatisierung zu erschließen. Durch volle Integration in bereits getätigte Investitionen erzielen diese, auf der Managementsoftware Empirum basierende Lösungen in kürzester Zeit messbare Mehrwerte in den betrieblichen Abläufen des Kunden.

Empirum ist heute das Kerngeschäft der matrix42 AG. Grundlage Empirums war vor mehr als 10 Jahren eine für ein Großprojekt entwickelte Lösung zur dynamischen Softwareinstallation in gesicherten Umgebungen. Zu dieser Zeit existierte am Markt keine adäquate Lösung, um die an uns gestellten Anforderungen zu erfüllen. Ziel war es, in dem aufkommenden WindowsNT-Umfeld mit den eingeschränkten Benutzerrechten Software automatisiert zu verteilen und individualisiert zu installieren. Die entstandene Lösung wurde konsequent weiterentwickelt und 1996 so mächtig, dass daraus ein eigenständiges Produkt wurde. Im Laufe der Jahre entstand aus dem Softwareverteilungs-Tool eine mächtige und umfassende Device-Lifecycle Lösung – Empirum PRO

Im Jahre 2007 fügten wir die Empirum Security Suite unserem Produktportfolio hinzu. Die Empirum Security Suite bietet einen völlig neuen Ansatz zum Schutz von Unternehmen durch externe und interne Angriffe und ermöglicht die Durchsetzung von Unternehmensrichtlinien. Es ist das erste pro-aktive, automatische Echtzeit-Abwehrsystem mit Funktionen wie Anwendungsüberwachung, Kontrolle externer Speichergeräte, Host-Intrusion-Prevention-System, einer Netzwerk- Firewall und WLAN-Überwachung.

Um eine marktgerechte Ausrichtung und einen Ausbau des Technologievorsprungs zu gewährleisten, wird die Weiterentwicklung Empirums zu einem großen Teil von unseren Kunden, Partnern und den Praxis-Erfahrungen unserer Consultants bestimmt. Auf diese Weise sichern wir langfristig den Erfolg von Empirum und bieten unseren Kunden ein auf ihre Bedürfnisse zugeschnittenes Produkt, welches durch neue Funktionen weitere Prozessoptimierungs- und Einsparungspotentiale bietet.

2. Über Empirum Security Suite

2.1. Einführung

Die Empirum Security Suite bietet einen völlig neuen Ansatz zum Schutz von Unternehmen vor externen und internen Angriffen. Es ist das erste proaktive, automatische Echtzeit-Abwehrsystem mit Funktionen wie Anwendungsüberwachung, Kontrolle externer Speichergeräte, Intrusion-Prevention-System, einer Netzwerk-Firewall und WLAN-Überwachung.

Die Mehrzahl der Unternehmen hat heute Antiviren-Lösungen im Einsatz. Ungeachtet dessen erleiden 68% aller großen Unternehmen regelmäßig erheblichen Schaden durch Viren und Denial-of-Service-Angriffe. Schutz gegen bekannte Bedrohungen und Sicherheitslücken bieten die meisten Antiviren- und Security-Produkte. Die Sicherheits-Lösung von matrix42 schützt hingegen auch vor unvorhergesehenen Angriffen. Die Empirum Security Suite benötigt keine Updates von (Viren-) Signaturen, um jederzeit einen vollständigen und integrierten Schutz vor Angriffen gewährleisten zu können.

Hinzu kommt, dass Mitarbeiter heute – gewollt oder ungewollt – eine große Bedrohung für das Unternehmensnetzwerk und die Sicherheit von vertraulichen Informationen darstellen. Der fast überall verfügbare Zugang zum Internet, verbunden mit der Nutzung von P2P und Instant-Messaging, sowie der unbewussten Installation von Spyware wird zu einer immer größeren Gefahr für die Sicherheit im Unternehmen. Diebstahl von vertraulichen Informationen mittels Keylogging oder externer Speichergeräte ist bereits heute Realität.

Angriffsversuche auf das Unternehmensnetzwerk nehmen stetig weiter zu und werden immer intelligenter. Über viele verschiedene Wege wird versucht, Kontrolle über Computer und Server zu erlangen, vertrauliche Informationen zu erhalten und das Unternehmen zu schädigen. Um einen effektiven Schutz gegen verschiedenste Angriffsversuche zu gewährleisten, ist eine umfassende Sicherheitslösung notwendig, die unterschiedliche Ebenen integriert überwacht. Dazu gehören Netzwerkzugriffe, Betriebssystemaktivitäten, Verhalten von Anwendungen und Nutzung externer Speichergeräte. Empirums einzigartige Sicherheitstechnologie überwacht und kontrolliert alle diese Ebenen und gewährleistet so jederzeit einen vollständigen und automatischen Schutz vor Angriffen.

Mit der Kombination aus einfachem, zentralem Management und umfassender verteilter Sicherheit und Kontrolle ist die Empirum Security Suite der Durchbruch im Bereich Unternehmenssicherheit.

Empirum Security Suite – 360° Endpoint Security

2.2. Wie schützt die Empirum Security Suite Ihr Unternehmen?

Die Sicherheitsinfrastruktur eines Unternehmens sollte verschiedene Sicherheitsebenen enthalten. Dazu gehören beispielsweise Netzwerk-Firewalls, konventionelle signaturbasierte Antiviren-Lösungen so wie Authentifizierungs- und Verschlüsselungssysteme.

Die Empirum Security Suite sollte als eine übergreifende Sicherheitsebene dieser Sicherheitsinfrastruktur betrachtet werden. Sie ergänzt die vorhandenen Sicherheitslösungen im Unternehmen und bietet einen proaktiven automatischen Schutz vor internen und externen Angriffen. Dies beinhaltet sowohl bekannte, als auch und unbekannt Bedrohungen.

ESS und IT-Grundschutz nach BSI

ESS vereinfacht die Administration der Sicherheitsfunktionen der Clients

Alle Funktionen sind vollständig in einer Suite verfügbar. Das komplette Management erfolgt zentral aus einer einzigen Konsole heraus. Auf den Computern im Unternehmen wird nur ein Agent benötigt, der alle Sicherheitsfunktionen abdeckt.

ESS sichert die Umsetzung von Compliance- und Sicherheitsrichtlinien

Die Anforderungen bezüglich der Compliance im Unternehmen sind abhängig von vorhandenen Unternehmensrichtlinien und bestehenden rechtlichen Vorschriften wie BSI-Grundschutz, Sarbanes-Oxley-Act (SOX) oder Basel II. Die Empirum Security Suite ermöglicht die Durchsetzung und Einhaltung der geforderten Standards und Richtlinien sowohl für die Computer im Unternehmen als auch für die mobilen Mitarbeiter und Produktübergreifend in einer Konsole (z.B. Kontrolle externer AV-Signaturen, Stand des Patchmanagements etc.).

ESS beschützt Computer vor unbekanntem Bedrohungen

Die Empirum Security Suite bietet einen automatischen, proaktiven Schutz für Computer gegen bekannte und unbekanntem Bedrohungen. Sie kann gefährliches Verhalten auf dem Computer entdecken und blockieren. Firewall, IDS/IPS und Gateway Antivirus bieten notwendige Barrieren gegen externe Bedrohungen. Diese bieten jedoch nur unzureichenden Schutz bei mobilen Computern von Außendienstmitarbeitern außerhalb des Unternehmens. Zusätzliche Probleme entstehen, wenn Bedrohungen nicht auf Netzwerkebene identifiziert und gefiltert werden können.

ESS ergänzt signaturbasierte Antivirenlösungen

Die Empirum Security Suite ergänzt signaturbasierte Antivirenlösungen, die lokal auf dem Computer installiert sind. Antivirenlösungen blockieren Angriffe von bekannten Viren und können infizierte Systeme von Viren reinigen. Leider setzt diese Art von Schutz voraus, dass eine Signatur für den Virus verfügbar ist, bevor der Virus erkannt und der Computer geschützt werden kann. Diese Verzögerung bis zur Verfügbarkeit und Installation neuer Signaturen öffnet ein Zeitfenster, in dem Computer vor neuen Viren ungeschützt sind. Eine signaturbasierende Antivirenlösung kann daher auch keinen Angriff stoppen, bei dem ein Virus von einem Angreifer speziell für ein Unternehmen entwickelt wurde. Diese programmierten, heimlichen Angriffe führen nie zur Veröffentlichung einer Signatur, da die Hersteller von Antivirenlösungen nicht davon erfahren.

ESS sichert die Durchsetzung von Softwarebezogenen Unternehmensrichtlinien

Anwendungen, die direkt von den Benutzern für persönliche Zwecke installiert werden, ohne vom Unternehmen freigegeben zu sein, können sowohl eine Bedrohung, als auch eine Quelle für Produktivitätsverluste sein. Die Empirum Security Suite bietet verschiedene Funktionen, um die Unternehmensrichtlinien in Bezug auf die Nutzung der Computer zu kontrollieren und durchzusetzen.

ESS liefert Informationen über verdächtige Aktionen

Die Empirum Security Suite liefert eine große Anzahl von Informationen über gefährliche oder verdächtige Aktionen, die den Computer bedrohen können. Diese Informationen ergänzen die Daten der Netzwerkmonitoring-Systeme, die im Rahmen einer IT-Sicherheitsinfrastruktur meist im Unternehmen vorhanden sind.

ESS verstärkt die Sicherheitsinfrastruktur

Die Sicherheit der IT-Systeme ist eine Kombination von vielen Faktoren, bei der die Technologie eine der Schlüsselkomponenten darstellt. Moderne Informations- und Kommunikationssysteme sind so komplex und offen nach außen, dass ihr Schutz nicht durch eine einzige Sicherheitstechnologie sichergestellt werden kann.

3. Aufgabenstellung / Allgemein

3.1. IT-Grundschutz nach BSI

In den IT-Grundschutz-Katalogen werden Standard-Sicherheitsmaßnahmen für typische Geschäftsprozesse, Anwendungen und IT-Systeme empfohlen. Ziel des IT-Grundschutzes ist es, einen angemessenen Schutz für alle Informationen einer Institution zu erreichen. IT-Grundschutz verfolgt dabei einen ganzheitlichen Ansatz. Durch die geeignete Kombination von organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmaßnahmen wird ein Sicherheitsniveau erreicht, das für den normalen Schutzbedarf angemessen und ausreichend ist, um geschäftsrelevante Informationen zu schützen. Darüber hinaus bilden die Maßnahmen der IT-Grundschutz-Kataloge nicht nur eine Basis für hochschutzbedürftige IT-Systeme und Anwendungen, sondern liefern an vielen Stellen bereits höherwertige Sicherheit.

Im Rahmen dieser Analyse soll untersucht werden, wie mit Hilfe der Empirum Security Suite IT-Sicherheitsrichtlinien durchgesetzt werden können, die im Rahmen der Umsetzung von IT-Grundschutz empfohlen sind.

Sämtliche Analysen basieren auf den Grundschutzkatalogen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) mit Stand Dezember 2007.



4. Betrachtung

Die Vorgehensweise nach IT-Grundschutz erfolgt nach einem Schichtenmodell, wobei mit zunehmendem Detailierungsgrad die Schichten

- Übergreifende Aspekte
- Infrastruktur
- IT-Systeme
- Netze
- IT-Anwendungen

betrachtet werden. Die Modellierung erfolgt umfassend auf den zuvor erhobenen und festgestellten IT-Verbund der Organisation.

Zu jedem Teil des Verbundes ergeben sich nach Untersuchung der einzelnen Schichten individuelle Gefährdungen und darauf anzuwendende empfohlene Maßnahmen.

Die Empirum Security Suite wurde entwickelt, um am Arbeitsplatz auf Geräte- und Anwendungsebene die im Rahmen des IT-Sicherheitskonzepts definierten Richtlinien wirksam umzusetzen. Darüber hinaus ist die ESS mit Funktionen zur Verschlüsselung und Netzwerksicherheit ausgestattet.

ESS und IT-Grundschutz nach BSI

5. Modellierung

Im Folgenden wird die Abdeckung der Gefährdungen und empfohlenen Maßnahmen durch die Empirum Security Suite auf den einzelnen Schichten des Modells erläutert. Gefährdungsmodul sind dabei durch ein G und Maßnahmenmodule durch ein M gekennzeichnet.

5.1. Übergreifende Aspekte

5.1.1. Organsiatorische Mängel

G 2.1: Gefahr durch unzureichende Regelungen. Dieser Gefahr wird keine Funktion der ESS entgegen gesetzt, jedoch erleichtert der Einsatz der ESS die methodische Erarbeitung und Anwendung von Regeln.

G 2.7: Unerlaubte Ausübung von Rechten, wozu auch die Ausführung von Anwendungen zählen. Die Anwendungsregeln der ESS definieren, welche Anwendungen an einzelnen oder Gruppen von Arbeitsplätzen ausgeführt werden dürfen und mit welchen Daten diese Anwendungen verknüpft werden können.

G 5.2: Vorsätzliche Manipulation an Daten oder Software. Durch Kryptographie und Anwendungsregeln kann definiert werden, dass Daten nur mit den zugehörigen Anwendungen bearbeitet werden dürfen. Log-Mechanismen innerhalb dieser Anwendungen ermöglichen dann die Kontrolle über Datenveränderungen. Die Manipulation über Betriebssystemwerkzeuge oder anderen, nicht freigegebene Anwendungen ist dann nicht möglich.

M 2.2: Betriebsmittelverwaltung. Durch die Device-Kontrolle innerhalb der ESS kann der Zugriff auf Wechseldatenträger richtliniengetreu gesteuert werden. USB-Massenspeicher können in Pools verwaltet werden, durch die automatische Verschlüsselung von USB-Massenspeichern kann gewährleistet werden, dass wichtige Daten die Organisation nicht verlassen. Die Entschlüsselung kann nur auf bekannten Arbeitsplätzen erfolgen.

5.1.2. Kryptokonzept

Die ESS kann Teil eines unternehmensweiten Verschlüsselungskonzept werden und richtlinienbasiert die Verschlüsselung auf definierten Datenträgerbereichen oder mobilen Datenträgern und Arbeitsplätzen erzwungen werden.

M2.166 Regelung des Einsatzes von Kryptomodulen.

M4.29 Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme. Tragbare IT-Systeme sollten zwingend mit einem geeigneten Verschlüsselungsprodukt ausgestattet sein. Die Verschlüsselung muss sich dabei in das übergeordnete Kryptokonzept einpassen.

M4.41 Einsatz angemessener Sicherheitsprodukte für IT-Systeme.

5.1.3. Hard- und Software Management

M2.216 Genehmigungsverfahren für IT-Komponenten. Durch die Device-Kontrolle der ESS kann die Nutzung einzelner IT-Komponenten und insbesondere Wechseldatenträger richtliniengetreu geregelt werden.

M2.218 Regelung der Mitnahme von Datenträgern und IT-Komponenten. Mit Hilfe der ESS-Devicekontrolle in Verbindung mit dem Kryptomodul kann die Nutzung von Wechseldatenträgern und insbesondere USB-Wechselmedien genau reglementiert werden (siehe auch M 2.2 Betriebsmittelverwaltung).

5.2. IT-Systeme

5.2.1. Clients

G5.4 Diebstahl. Lokal gespeicherte Daten sind durch Diebstahl mobiler Arbeitsplätze gefährdet und sollten daher durch ein Kryptokonzept wirkungsvoll gesichert sein.

G5.9 Unberechtigte IT-Nutzung. Jeder Anwender soll gemäß der IT-Sicherheitsrichtlinien die ihm zur Benutzung überlassenen IT-Systeme nur in dem zur Aufgabenerfüllung erforderlichen Umfang nutzen können und dürfen. Die ESS sorgt durch die Device- und Anwendungs-Kontrolle für die Umsetzung dieser Forderung.

M4.29 Einsatz eines Verschlüsselungsproduktes für tragbare IT-Systeme.

M4.41 Einsatz angemessener Sicherheitsprodukte für IT-Systeme.

5.3. Netze

5.3.1. Netze allgemein

G5.9 Unberechtigte IT-Nutzung. Analog zur Richtlinie für die Arbeitsplätze gilt die Forderung der geregelten Nutzung der Netzwerkressourcen. Die integrierte Firewall kann durch die zentrale Steuerung der Firewall-Richtlinien diese Regeln auf Paketebene wirkungsvoll durchsetzen.

5.3.2. WLAN

Die Devicekontrolle der Empirum Security Suite bietet die Steuerung der Nutzung von WLAN's am Arbeitsplatz. Die Richtlinien berücksichtigen dabei die jeweiligen Einsatzorte sowie Art der WLAN-Nutzung. Individuell können die zum Einsatz kommenden Verschlüsselungsrichtlinien definiert werden, so dass keine unverschlüsselte Kommunikation zu Stande kommen kann. Auch die Nutzung von öffentlichen Zugangspunkten (Hot-Spots) wird in der Regelung berücksichtigt.

G2.118 Unzureichende Regelungen zum WLAN-Einsatz.

G2.119 Ungeeignete Auswahl von WLAN-Authentisierungsverfahren.

G2.120 Ungeeignete Aufstellung von sicherheitsrelevanten IT-Systemen.

G2.121 Unzureichende Kontrolle von WLANs.

G3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen.

G4.60 Unkontrollierte Ausbreitung der Funkwellen.

G5.138 Angriffe auf WLAN-Komponenten.

G5.139 Abhören der WLAN-Kommunikation.

M2.383 Auswahl eines geeigneten WLAN-Standards.

M4.293 Sicherer Betrieb von Hotspots.

M4.295 Sichere Konfiguration der WLAN-Clients.

M4.297 Sicherer Betrieb der WLAN-Komponenten.

ESS und IT-Grundschutz nach BSI

5.4. Anwendungen

5.4.1. Mobile Datenträger

G4.52 Datenverlust bei mobilem Einsatz.

G5.9 Unberechtigte IT-Nutzung. Die Kontrolle über die Nutzung mobiler Datenträger und USB-Medien muss in der IT-Sicherheitsrichtlinie definiert werden. Durch die Richtlinie wird das Risiko minimiert, dass vertrauliche Daten auf undefinierten Wegen die Organisation verlassen. Der Einsatz mobiler Datenträger sollte dann auch mit dem Einsatz geeigneter Kryptoverfahren gekoppelt sein.

G3.3 Nichtbeachtung von IT-Sicherheitsmaßnahmen. Durch geeignete technische Maßnahmen muss sicher gestellt sein, dass definierte Richtlinien nicht leichtfertig oder bewusst umgangen werden können.

G5.141 Datendiebstahl über mobile Datenträger.

M4.200 Umgang mit USB-Speichermedien.

M4.232 Sichere Nutzung von Zusatzspeicherkarten.

M4.34 Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen Betrieb.

M2.218 Regelung der Mitnahme von Datenträgern und IT-Komponenten.

M2.401 Umgang mit mobilen Datenträgern und Geräten.

M4.4 Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern.

6. Zusammenfassung

Zusammenfassend kann gesagt werden, dass die Empirum Security Suite im Rahmen ihrer Funktionalität einen hohen Erfüllungsgrad bei der Umsetzung zentraler IT-Sicherheitsrichtlinien für den Arbeitsplatz, insbesondere der Geräte- und Anwendungskontrolle bietet.

Der Einsatz der Empirum Security Suite unterstützt das IT-Sicherheitsmanagement direkt bei der Umsetzung der empfohlenen Maßnahmen zur Erreichung der Schutzziele gemäß der ISO 27001.