Gesamtheitliches IT-Notfall-Management

iQSol

Security made in Austria.

Gesamtheitliches IT-Notfall-Management

Security-Lösungen und -Prozesse zur Wahrung der Business Continuity

E-Book

Inhalt

IT-Notfall-Management: Software hilft!

69 Prozent aller deutschen Industrieunternehmen sind bereits Datendiebstahl, Spionage und Sabotage zum Opfer gefallen, in der Gesamtwirtschaft waren es immerhin 51 Prozent[1]. Wem jetzt noch nicht die Schweißperlen auf der Stirn stehen, der gehört wohl zu den ebenfalls 51 Prozent der deutschen Industrieunternehmen, die über ein Notfall-Management verfügen. Die restlichen 49 Prozent bleiben vor Datenabflüssen, der Unterbrechung der Business Continuity (BC) sowie vor zerstörten IT-Systemen bei Cyber-Angriffen ungeschützt.

Doch nicht nur das: Das aktualisierte Europäische IT-Sicherheitsgesetz fordert von führenden Unternehmen aus fast allen Branchen, dass Hacker-Angriffe oder sonstige sicherheitsrelevanten Vorfälle gemeldet werden. Doch was meldet man? Sind forensische Daten und gerichtsfeste Logs vorhanden? Oder bezahlt man besser die Strafe, bleibt anonym und erspart sich die öffentliche Blamage, weil man doch auf relativ niedrigem Sicherheitslevel unterwegs war?

Die Ereignisse um den Deutschen Bundestag[2] und viele weitere ähnliche Fälle zeigen, was bevorsteht: Die Security ist nicht up to date oder rasch überwunden, die Fehlersuche erweist sich als extrem aufwändig, die Kommunikation mit Betroffenen ist nicht vorhanden und der Extremfall – sprich: der Shutdown bzw. Restart der IT – gelingt nur mit feuchten Händen mittels „Steckerziehen".

Das Wettrüsten der hochspezialisierten US-Software-Konzerne gegen Angriffe und viele, aber niemals alle, potenziellen „Threats" zeigt vor allem, dass eine Zwei-Klassen-Gesellschaft entsteht: Jene, die sich diese Lösungen und Services leisten können, und jene, die relativ leicht zu Opfern werden. Dabei wird übersehen, dass Security ein integraler Prozess der gesamten Organisation und IT-Infrastruktur ist und auch für den Fall der Ausschaltung der besten Security-Tools ein „Plan B" existieren muss – nämlich in Form von Business-Continuity-Konzepten und Softwaretools.

Auch die Marktentwicklungen und Unternehmenskäufe in den USA zeigen, dass die Zukunft nicht in der x-ten Security-Software liegt, sondern in einer zentralen, offenen Security-Plattform sowie in nachgelagerten Tools, die Kommunikation und Incident-Response-Management beziehungsweise BCM-Aufgaben integrieren.

Im ersten Schritt hilft es bereits, wenn die linke Hand weiß, was die rechte tut – ein Notfallhandbuch macht es möglich! Wird dies durch zusätzliche, speziell für die Unternehmensanforderungen zugeschnittene Software gestützt, kann man darüber hinaus auch den gesetzlichen Bestimmungen gerecht werden.

Daten, die für Prüfungen oder Meldungen vorliegen müssen, sollten durch entsprechende Lösungen gesammelt, gespeichert und analysiert werden können.

Wie das gelingen kann, beschreiben wir in den nachfolgenden Beiträgen.

[1] Umfrageergebnisse des Digitalverbands Bitkom e. V.
[2] Informationen zum Cyberangriff auf den Bundestag: Abschlussbericht BSI:
https://netzpolitik.org/2016/wir-veroeffentlichen-dokumente-zum-bundestagshack-wie-man-die-abgeordneten-im-unklaren-liess/#abschlussbericht_bsi_20151103

Wie Log Management für (Rechts-)Sicherheit sorgt

Netzwerkgeräte, Server und Systeme geben permanent Signale ab, auch dann, wenn Änderungen an ihnen vorgenommen werden. Diese werden normalerweise als Logs, also in Form von Protokollen, festgehalten. Doch was tun mit diesen Protokollen? Es bedarf einer Log-Management-Lösung, die bestenfalls über Security Information & Event Management (SIEM)-Funktionen verfügt und somit zusätzlich Alarmierungs- und Eskalationsmöglichkeiten bietet.

Wofür werden Logs benötigt?

Zum einen sind Logs notwendig, um Compliance-Richtlinien einzuhalten oder Audits von Wirtschaftsprüfern zu überstehen. Mit dem aktualisierten Europäischen IT-Sicherheitsgesetz, das 2015 verabschiedet wurde, sind zudem Kritische Infrastrukturen (KRITIS[3]) wie bspw. Stromversorger und andere Unternehmen, die das Gemeinwohl betreffen, verpflichtet, dem Gesetzgeber Vorkommnisse an ihrer IT zu melden.

Dies gelingt aber nicht ohne Archiv, das die revisionssichere Speicherung aller Events auch über einen längeren Zeitraum hinweg zulässt. Und: Wo unterschiedliche Systeme, da unterschiedliche Formate. Logs müssen zunächst korreliert werden, damit eine einheitliche Auswertung der Daten ermöglicht wird.

Zum anderen helfen Logs Unternehmen, eigenständig Events an den Systemen nachzuvollziehen und bei unerwünschten Bewegungen einzugreifen. Das ist gerade bei Zugriffen durch Hacker auf die Systeme wertvoll.

Aber wie bekommen Betroffene mit, dass etwas geschieht? Das Log-Management-System muss in einem solchen Fall mit einer Alarmierung verknüpft werden, die in Echtzeit korreliert und informiert. Diese Verbindung nennt sich dann SIEM.

Im Falle der Abwehr von Ransomware-Bedrohungen zum Beispiel würde ein verlässlicher Security-Berater oder -Anbieter dafür sorgen, dass mit Microsoft-Bordmitteln[4] bereits ein guter allgemeingültiger Schutz aufgebaut werden und mit einer SIEM-Lösung die Feinheiten, die Alarmierung sowie die Erkennung ähnlich gestrickter Fälle erfolgen kann.

[3] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und Bundesamt für Sicherheit in der Informationstechnik; Sektoren und Branchen Kritischer Infrastrukturen:
http://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Sektoren/sektoren_node.html
[4] Playbook #2 - Windows Advanced Security:
http://www.iqsol.biz/news/news-detail/playbook-2-windows-advanced-security/

Was tut also ein Log-Management-System?

Eine Log-Management-Lösung kann per Hardware-Appliance oder als Virtuelle Maschine (VM) direkt im Unternehmen installiert oder oftmals auch als Managed-Security-Service bezogen werden. Dazugehörige Log-Agenten werden an Server und Applikationen angebunden und spielen dann nach vorher definierten Regeln sämtliche Logs und Events verschlüsselt zunächst in die Log-Management-Lösung, dann in ein Langzeitarchiv sowie auf einen Enterprise-Reporting-Server, wo detaillierte Compliance-Reports erstellt werden. Über ein Dashboard können sämtliche Bewegungen überwacht werden.

Zusatzfunktionalität für Zusatzschutz

Log-Management-Systeme können um verschiedene Funktionen erweitert werden. Zum Beispiel sind sogenannte Honeypots ratsam. Die „Honigtöpfe“ verfolgen das Ziel, Angreifer von den eigentlichen Systemen abzulenken und somit Schäden an Produktionssteuerungsanlagen, medizintechnischen Umgebungen und anderen sicherheitskritischen Systemen zu verhindern.

Ebenso ist es ratsam, auf Schwachstellen-Scans zu setzen. Das Ziel hierbei ist es, bestimmte Hosts bzw. Netzwerksegmente zu definierten Zeiten auf Schwachstellen zu überprüfen. Weitere vorhandene Sensoren können ebenso problemlos eingebunden werden.

Das Log Management archiviert also nicht nur Logs und informiert, wenn Trojaner, Viren, Hacker sich an den Systemen zu schaffen machen – es ist sogar in der Lage, Prävention zu unterstützen. Log Management sorgt somit für Sicherheit auf rechtlicher, aber auch auf technischer Seite.

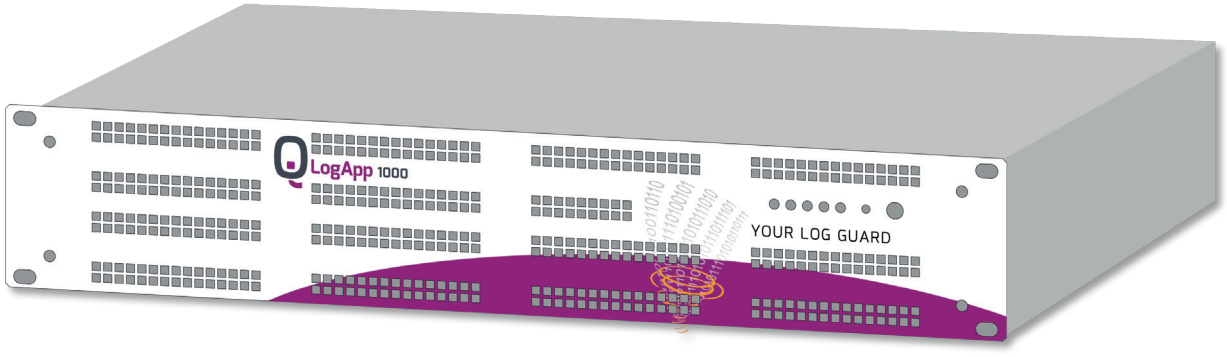
LogApp

Security Information & Event Management

Der Sherlock Holmes für unerwünschte Vorkommnisse an Ihrer IT!

- Log-Quellen überwachen und auswerten
- Langzeitarchivierung nach Compliance-Vorgaben
- Analyse, Korrelation und Reporting
- SIEM-Funktionalität
- Risikobewertung und Schwachstellenscans
- als Appliance, VM oder Managed-Security-Service verfügbar

Webinar LogApp mit dem Chefentwickler persönlich! Betreff „LogApp“ an office@iqsol.biz



iQSol GmbH
Oed 119
A - 3312 Oed

T: +43 7472 207 67
E: office@iqsol.biz

www.iqsol.biz

Eingriff bei Angriff: Alarmierung für Echtzeitschutz

Damit ein IT-Notfall-Management greifen kann, muss zunächst einmal Kenntnis darüber vorliegen, dass ein Notfall eingetreten ist. Viele Unternehmen bekommen dies aber erst mit, wenn plötzlich das System nicht mehr reagiert, einzelne Rechner streiken, Dateien verschlüsselt sind (Ransomware) oder andere Maschinen ausfallen. Ist es soweit erst einmal gekommen, sind Schäden bereits angerichtet und Angreifer hatten deutlich zu lange Zeit, um zum Beispiel sensible Daten auszuspionieren.

Branchenweiter Bedarf an Unternehmensalarmierung

Wer verhindern möchte, dass Angriffe unbemerkt vonstattengehen, benötigt eine Lösung zur Unternehmensalarmierung, die warnt, sobald Auffälligkeiten an Servern, Systemen oder Applikationen auftreten. Damit bleibt genug Zeit, Schlimmeres zu verhindern, indem bestimmte Schutzmechanismen, beispielsweise festgehalten in einem Notfallhandbuch, angestoßen werden und schnell greifen.

Stellt man sich zum Beispiel vor, dass in der industriellen Produktion nicht nur wichtige Maschinen aufgrund eines Hackerangriffs stillstehen, sondern wegen eines Trojaners zudem geheime Daten in die falschen Hände gelangen, wird die Wichtigkeit einer Alarmierung schnell klar. Seien es Automodell-Pläne, geheime Konto- oder geschützte Personendaten – fast jedes Unternehmen verwaltet schützenswerte und gewinnbringende Informationen.

Krisensituationen, die alle betreffen

Um noch größere Sicherheit zu bieten, kann in manchen Fällen sogar ein Schutz für Leib und Leben per Alarmierung bereitgestellt werden. Bricht ein Feuer aus, ist mit Überschwemmungen zu rechnen oder treten giftige Gase aus, muss die ganze Mannschaft evakuiert werden. Auch dies kann eine Unternehmensalarmierung leisten, indem in spezifischen Fällen Nachrichten und Handlungsanweisungen an alle ausgesendet werden.

Was tut also ein Alarmierungssystem?

Üblicherweise arbeiten solche Alarmierungssysteme, angebunden an Log-Management- oder andere Sicherheitslösungen, nach vordefinierten Regeln und Abläufen, sogenannten Eskalationsprozeduren. Ist etwas nicht so, wie es vorkonfiguriert wurde oder werden Schwellwerte überschritten, erfolgt eine Alarmierung – sei es telefonisch, per E-Mail oder per Sprachnachricht.

Die richtige Anlaufstelle ist hier natürlich der IT-Administrator, der über das gesamte Netzwerk verfügt. Ist er nicht da, muss seine Vertretung erreichbar sein, die sich dann der Sicherheitsaufgabe annimmt. Auch sie sollten in einer entsprechenden IT-Lösung mit all ihren Kontaktdaten hinterlegt sein – ebenso wie Feiertage oder Dienstpläne, die im Falle einer Alarmierung beachtet werden. In besonderen Fällen, u. a. bei Feueralarm(-Übungen), spricht die Lösung alle anwesenden Mitarbeiter an.

Für die Nachweisbarkeit und auch die Nachvollziehbarkeit empfiehlt sich zudem die Anbindung des Systems an vorhandene Monitoring-Lösungen, Leitstellen-Applikationen und natürlich das globale Service-Management unter Beachtung der verschiedenen Zuständigkeiten und Zeitverschiebungen („Follow-the-Sun"-Konzept).

Um Hochverfügbarkeit zu erreichen, empfiehlt es sich außerdem, sowohl Hard- als auch Software zu duplizieren und das gesamte System somit redundant aufzubauen. Der Ausfall einer Komponente wird dann durch das zweite System aufgefangen.

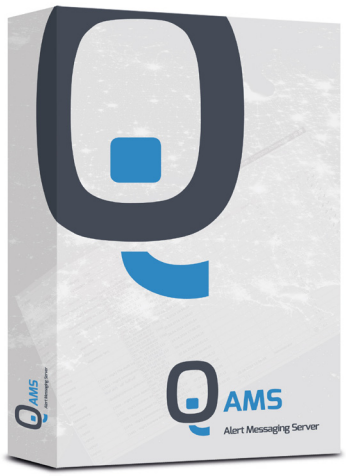
AMS

Alert Messaging Server

Der Wachhund für Hochverfügbarkeitsumgebungen!

- Angreifer und Störungen an Systemen in Echtzeit erkennen
- Alarmierung per E-Mail, Anruf oder SMS
- integrierte Dienstpläne und Eskalationsprozeduren
- modular und vollständig anpassbar
- Schnittstellen zu Monitoring-Lösungen
- als Appliance, VM oder Managed-Security-Service verfügbar

Webinar Alerting mit dem Chefentwickler persönlich! Betreff „AMS“ an office@iqsol.biz



iQSol GmbH
Oed 119
A - 3312 Oed

T: +43 7472 207 67
E: office@iqsol.biz

www.iqsol.biz

Notfallplan und Desaster-Test: Vorbereitung ist alles!

Tritt im Unternehmen ein Stromausfall ein, bricht oft genug das Chaos los: Es ist unklar, welche Schritte eingeleitet werden müssen und wer dafür Sorge trägt; eine mangelnde Übersicht über im Unternehmen eingesetzte Soft- und Hardware sowie deren Abhängigkeiten erschwert die Problemlösung darüber hinaus erheblich.

Die Folge: ein totaler Blackout, der Zeit, Geld, Daten und Renommee kostet.

Fakten sammeln

Ein Notfallhandbuch[5] sorgt hier für Klarheit. In ihm werden nicht nur sämtliche Geräte und ihre Abhängigkeiten aufgeschlüsselt, sondern auch Zuständigkeiten definiert. Wichtig ist, dass eine regelmäßige Pflege stattfindet, d. h. immer dann, wenn auch nur eine Kleinigkeit im Netzwerk verändert wird, muss diese Information innerhalb des Handbuchs hinterlegt werden. Was kleinlich klingt, kann in Notsituationen Maschinen und Daten retten, die durch einen Stromausfall, zum Beispiel durch einen Blitzeinschlag oder eine nicht funktionierende Kühlung, oder, im Falle der Daten, durch ein kaputtes Zahnrad im System bedroht sind.

Power Management: Shutdown, Restart, Recovery

Die Abhängigkeit von Unternehmen von einer funktionierenden Stromversorgung ist evident. Kein Rechner, kein Server läuft länger, als es der Akku oder die Unterbrechungsfreie Stromversorgung (USV) erlaubt. Auch Generatoren sind kein Pferd, auf das man sicher setzen kann, denn wurde der Diesel nicht nachgefüllt und der Ausfall hält länger an, sitzen Firmen schnell im Dunkeln. Damit verbunden ist nicht nur eine unterbrochene Arbeitsleistung (Business Continuity), sondern auch ein Datenverlust, wenn sich Server und Systeme letztlich einfach selbst ausschalten.

Gelöst wird das durch eine Power-Management-Lösung: Sie wird in die IT-Infrastruktur integriert und erlaubt es auf Basis des USV-Status sowie der Umgebungssensoren, Server geordnet herunterzufahren; ist die Gefahrensituation überwunden, funktioniert auch der Restart aller Maschinen auf Knopfdruck. Darüber hinaus sind auch Datenmigrationen in ein zweites Rechenzentrum denkbar, um durch Redundanz zusätzliche Sicherheit zu schaffen.

Natürlich geht ein funktionierendes, auf Abhängigkeiten und logische Abläufe konzentriertes Power Management weit über gängige USV-Monitoring-Lösungen der Hersteller hinaus. Ein organisatorischer Ansatz aus der Sicht des Betriebs von Software- und Hardware-Infrastruktur sorgt dafür, dass zum Beispiel auch virtuelle Systeme, Datenbanken und Netzwerkdienste genauso integriert sind wie eben USV-Anlagen und Notstrom-Aggregate.

---

[5] Musterhandbuch:
http://www.notfallhandbuch.at/musterhandbuch/

Die Abbildung vieler möglicher Szenarien („Wenn-Dann"-Bedingungen) gibt also volle Handlungsfähigkeit, wenn der Countdown läuft und die USV-Anlagen doch schneller ausfallen als errechnet und eigentlich geplant. Teilabschaltungen von Servergruppen, Datenevakuierung in Ausweichrechenzentren und Priorisierung von Diensten sind nur einige Stichworte, die zeigen sollen, dass umgesetzte Planungen durch Software-Einsatz Schaden nachweislich abwenden.

Übung macht den Meister

Ebenfalls ratsam sind sogenannte Desaster-Tests. Mit ihnen wird genau das Vorgehen geübt, das in dem bereits besprochenen Notfallhandbuch festgelegt wurde. Auch Auditoren verlangen zunehmend mehr als Konzepte und Gedankenspiele, sie wollen reale Tests, Auswertungen und Analysen sehen, um die Risiken einschätzen zu können: Wirtschaftsprüfer, Aufsichtsbehörden, Versicherer, Datenschützer – die Liste wird wöchentlich länger.

Es gibt kaum ein IT-Betätigungsfeld, in dem Fehleinschätzungen und nicht vorhandene Planungen so dramatische Auswirkungen zeigen wie beim Thema Desaster Recovery, Shutdown und Wiederanlauf sowie bei der Datenwiederherstellung. Wo Natur, der Mensch, die IT und die Physik unter Zeitdruck so geballt aufeinander treffen, ist erfahrungsgemäß Undenkbares eher die Regel als die Ausnahme.

Die klassischen Fälle aus der Praxis sind u. a.:

- USV-Durchhaltevermögen kürzer als angenommen
- Leitungen und Steckerverbindungen defekt
- korrodierte USV-Anlagen
- Ausfall von Klimaanlagen
- mehrfache Stromausfälle und wiederholte Starts
- Dieselprobleme, Aggregate fahren nicht hoch
- Bedienungspersonal nicht vorhanden/greifbar (Schlüssel etc.)
- Naturkatastrophen und Kaskadeneffekte (zwei Faktoren)
- Ursachen für Fehlalarme können nicht beseitigt werden

Eine Probe aufs Exempel hilft somit dabei, eventuelle Mängel am definierten Procedere aufzudecken und eine gewisse Gewohnheit einkehren zu lassen, die im Krisenfall für einen kühlen Kopf sorgt.

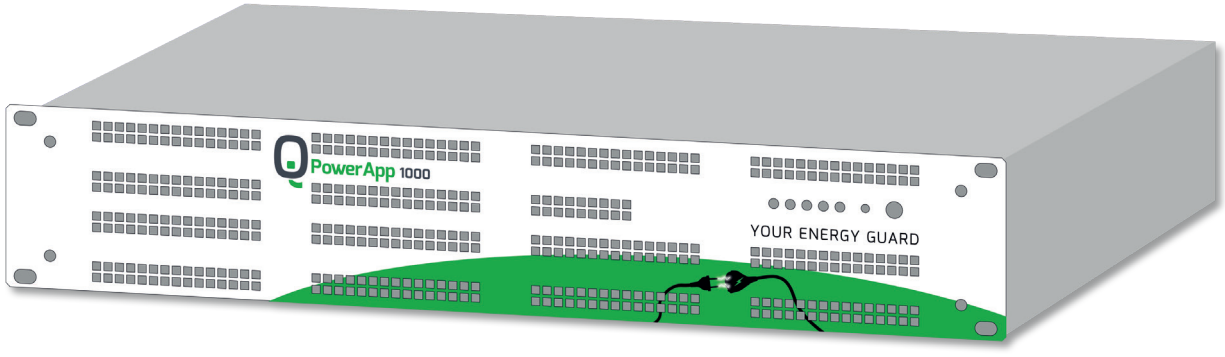
PowerApp

Your Energy Guard

Immer unter Strom dank USV-Power-Management!

- Sichern Sie Ihre Business Continuity
- Shutdown/Restart auf Knopfdruck
- Live-Migration virtueller Systeme
- Simulationen und Desaster-Tests
- Compliance durch Audittrails
- als Appliance, VM oder Managed-Security-Service verfügbar

Webinar
Power Management
mit dem Chefentwickler
persönlich!
Betreff „PowerApp“
an office@iqsol.biz



iQSol GmbH
Oed 119
A - 3312 Oed

T: +43 7472 207 67
E: office@iqsol.biz

www.iqsol.biz

Sicherheit 360°: Eine Plattform, große Wirkung!

Hochsicherheit – das ist der Wunsch, den viele Unternehmen hegen. Zu 100 Prozent kann dieser Wunsch niemals erfüllt werden, da fast täglich neue Bedrohungen für IT-Systeme auf den Plan treten, denen neu begegnet werden muss. Was man allerdings kann, sind die Rahmenbedingungen für den größtmöglichen Schutz zu schaffen, der Unternehmen bis zu 360° absichert. Denn was hilft es, wenn fünf, zehn oder 15 Security-Tools ausgeknockt wurden und der Schaden angerichtet ist, sei es durch gezielte Angriffe, Sabotage unzufriedener Mitarbeiter oder einfach durch Unachtsamkeit oder Sorglosigkeit.

Kombinationsvermögen zahlt sich aus: Security und BCM

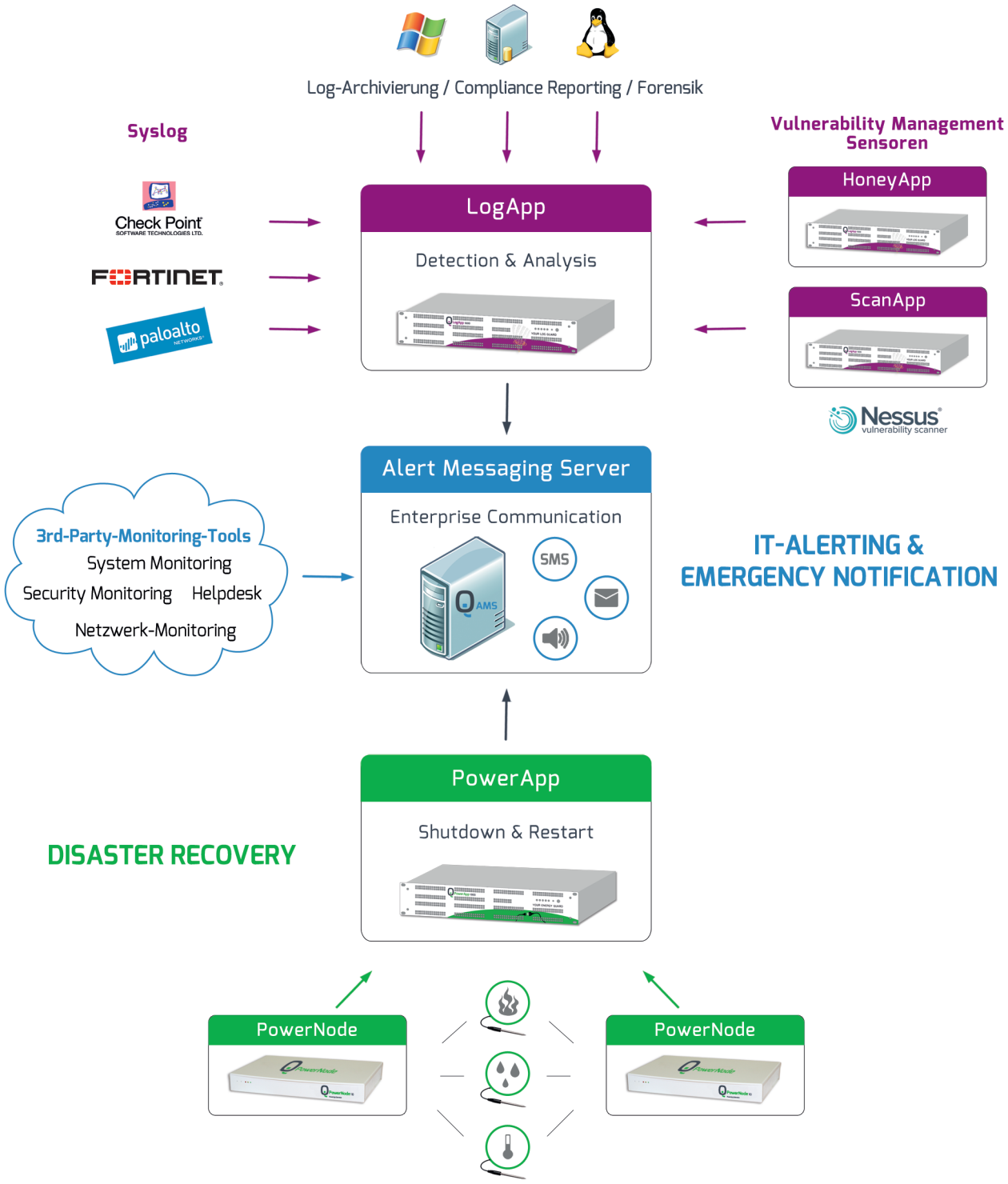
Fasst man die in diesem Dokument erläuterten Erkenntnisse zusammen, so wird deutlich: Die fast nahtlose Sicherheit kann nur dann gewährleistet werden, wenn man Log Management, Alarmierung und Power Management sinnvoll miteinander kombiniert. Denn schließlich bedingen sie sich gegenseitig: Muss eine IT-Infrastruktur stillgelegt werden, weil sonst Daten verlorengehen oder Geräte Schaden nehmen, erzeugt das Logs. Diese Logs müssen revisionssicher archiviert und ausgewertet werden. Und damit der IT-Admin erfährt, dass aktuell Protokolle über unerwünschte Aktivitäten geschrieben werden, wird die Alarmierung ausgelöst und er kann im Bedarfsfall korrigierend oder unterstützend eingreifen. Auch wollen User, Bürger und Mitarbeiter über Vorkommnisse informiert sein und bei Bedarf helfen.

Business Continuity sicherstellen

Das Ziel all dieser Vorkehrungen ist neben dem Schutz vor Angreifern vor allem die Aufrechterhaltung der Arbeitsfähigkeit: Das Business-Continuity-Management muss erreichen, dass alle Arbeitnehmer in der Lage sind, ihre Tätigkeiten weiter auszuführen, selbst, wenn der Strom doch einmal wegbleibt. Ist das nicht der Fall, muss es zumindest möglich sein, den Status von Servern und Systemen so beizubehalten, als sei nichts geschehen – um dann nach einem raschen Wiederanlauf dort weiterarbeiten zu können, wo man unterbrochen wurde.

SECURITY PROTECTION & DETECTION

LOG MANAGEMENT
SIEM (Security Information & Event Management)



BUSINESS-CONTINUITY-MANAGEMENT

Was die Zukunft bringt

Mit der zunehmenden Technologievielfalt und dem damit verbundenen Wachstum der Gefahren und Angriffsvektoren wird auch IT-Sicherheit immer komplexer. Betrachtet man beispielsweise den Bereich der „Internet of Things", in dem u. a. Maschinen-Sensordaten gesammelt und für Big Data weiter verwendet werden können, zeigt sich, welche Relevanz Produktionssicherheit hat: Sie ist ein unternehmenskritischer Faktor.

Wie aber begegnen Unternehmen dieser Herausforderung?

Ein zukunftsfähiger Weg sind Managed-Security-Services (MSS). Sie bieten die notwendige Flexibilität, um das Zusammenwachsen von Recht, Organisation und IT zu stemmen. Darüber hinaus gewährleisten sie eine größtmögliche Verfügbarkeit, ohne dass Unternehmen dabei mit eigenem, teurem IT-Personal 24/7 verfügbar sein müssen. Sie ermöglichen es, eine prozessorientierte, durchgängige Lösung aufzubauen, die zum Beispiel vom Firewall-Management bis zum Wiederanlauf all das abdeckt, was eine Business Continuity langfristig gewährleistet. Hier sind europäische Lösungen gefragt – auch und insbesondere aufgrund der Problematik des 2001 verabschiedeten US-amerikanischen Patriot Acts[6].

[6] Auswirkungen auf den Schutz personenbezogener Daten und geistigen Eigentums
https://de.wikipedia.org/wiki/USA_PATRIOT_Act#Auswirkungen_auf_den_Schutz_personenbezogener_Daten_und_geistigen_Eigentums

Fragen und Antworten

Unternehmen, Behörden oder Institutionen stehen oftmals vor einer gewaltigen Sicherheitsaufgabe bei beschränkten Ressourcen. Im Folgenden sollen einige Antworten auf die häufigsten Fragestellungen gegeben werden.

A) Spätestens 2017 wird es notwendig, Logs zu sammeln und vorzuhalten. Welche Aspekte sind zu berücksichtigen und welche Vorteile haben Cloud- und Managed-Service-Verträge?

Die Technologie ist schon viele Jahre verfügbar und ausgereift. Wenn nun an die Einführung gedacht wird, macht es Sinn, mit den wichtigsten Systemen (DNS, Windows, Firewalls etc.) zu beginnen und schrittweise zu erweitern. Viele Firewall-Hersteller haben hier noch Aufholbedarf was Monitoring, SIEM-Kompetenzen und Log-Archivierung angeht. Eine US-amerikanische Cloud-Lösung ist rasch implementiert, wird aber oft sehr teuer, da nach Bandbreiten etc. lizenziert wird und der Datenschutz nach neuesten EU-Anforderungen häufig nicht gewährleistet ist. Managed-Security-Services (MSS) bedeuten eine Auslagerung von Ressourcen, einen massiven Qualitätsanstieg und einen Ansprechpartner im Notfall zu überschaubaren Kosten. Ein guter MSS-Provider übernimmt auch Audits und das Firewall-Management sowie die gesamte Administration (Lizenzierung, Wartungen, Schulungen, Konfigurationen, Tests, Reporting) anderer Security-Hersteller.

B) IT wird immer mehr zur Chefsache und das Unternehmen in seiner Gesamtheit beruht auf der IT. Cyber-Versicherungen verlangen umfassende Audits und Nachweise, ebenso Wirtschaftsprüfer. Kann ich diese Anforderungen mit einer SIEM-Lösung und nachgelagerten BCM-Maßnahmen erfüllen?

Moderne SIEM-Lösungen können out-of-the-box oder nach individueller Anpassung alle geforderten Reports, Standards und Normen erfüllen. Je nach Themen und Branche können Zugriffe, Logs, Datenänderungen etc. protokolliert und archiviert werden. Vordefinierte Reports verkürzen Audits und die Software weist nach, wer was wann wo gemacht hat.

BCM-Maßnahmen sind leider noch selten und beschränken sich meist auf Notfallhandbücher, die rasch obsolet sind. Hier ist ein automatisierter, prozessorientierter Übergang von der Security-Plattform zu einer BCM-Plattform zu schaffen. Ein ultimativer „Outbreak"-Alarm aus einer SIEM-Lösung kann zur Folge haben, dass auf Knopfdruck (in einer Incident-Response-Lösung) die IT stillgelegt wird.

C) Im Grundschutzhandbuch und in anderen Ratgebern finden sich Punkte wie Notfallalarmierung, Wiederanlaufkonzepte und andere organisatorische Anforderungen für das Krisenmanagement. Macht es Sinn, hier auf Konzepte und Paperwork und/oder auf Software zu setzen?

Mit PowerApp und Alert Messaging Server sind auch die bisherigen Randthemen der Notfallalarmierung und des Desaster-Managements mehr als erfüllt. Hier stehen vor allem die Vorteile in der Praxis im Vordergrund, weniger die allgemeinen Anforderungen des Grundschutzhandbuches. Dies ist auch der Tatsache geschuldet, dass es sich bei PowerApp um ein neues Thema bzw. Produkt handelt.

Im Krisenfall selbst ist es immer vorteilhafter, nach umfassenden Planungen und Konzepten eine automatisierte und standardisierte Software im Einsatz zu haben und den Ablauf proaktiv zu organisieren. Software muss unter Strom laufen, dann tut sie, was sie tun muss. Regelmäßige Desaster-Tests sorgen darüber hinaus für die Verlässlichkeit.

Glossar

SIEM	Security Information & Event Management (SIEM) verfolgt das Ziel, die gesamte IT eines Unternehmens abzusichern. Dabei werden sicherheitsrelevante Daten von Servern und Geräten gesammelt, korreliert und ausgewertet. Besteht Gefahr, löst SIEM einen Alarm aus.
Events	sicherheitsrelevante Ereignisse in der IT-Umgebung
Logs	Informationen in Form von Protokollen von Geräten wie Servern, Applikationen, Datenbanken, Netzwerkgeräten oder Host-Systemen
Korrelation	Herstellen einer Beziehung zwischen verschiedenen Informationen, die aufeinander einwirken
Business Continuity	Betriebskontinuität bzw. durchgehende Geschäftsprozesse
Internet of Things	Computer werden durch kaum als Computer wahrnehmbare Gegenstände ersetzt, bspw. Wearables oder andere eingebettete Computer

Weitere Informationen

BSI-Standard 100-4, Notfallmanagement:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1004_pdf.pdf;jsessionid=2AB518B61DC6BC89A0C6EC9FF2BF49E5.2_cid359?__blob=publicationFile&v=1

Bildnachweise

Seite 2: Stethoskop auf Tastatur © Light Impression / fotolia.com
Seite 4: Time for plan B! © MK-Photo / fotolia.com
Seite 5: anfangen! © MK-Photo / fotolia.com
Seite 6: Wasps Eating Jam © vectorass / fotolia.com
Seite 7: Magnifying Glass © BillionPhotos.com / fotolia.com
Seite 8: touchscreen smartphone with security alarm on the screen © georgejmclittle / fotolia.com
Seite 10: Security CCTV camera in office building © alice_photo / fotolia.com
Seite 11: Blitzeinschlag in Frankfurt © Dream-Emotion / fotolia.com
Seite 13: Mediterranean Sea - Night © Guillaume Le Bloas / fotolia.com

Über die iQSol GmbH

Die iQSol GmbH setzt seit Gründung 2011 auf die Entwicklung und Bereitstellung von IT-Security-Lösungen, die die IT-Infrastruktur von Unternehmen absichern, für einen reibungslosen Betrieb sowie ein unterbrechungsfreies Arbeiten sorgen. Die Lösungen aus den Bereichen Alarmierung, Log und Power Management sind bei Kunden verschiedener Branchen in Österreich, Deutschland sowie Osteuropa im Einsatz.

Der Autor

Jürgen Kolb ist Managing Partner der österreichischen iQSol GmbH. Nach verschiedenen beruflichen Stationen in der öffentlichen Verwaltung sowie in der freien Wirtschaft gründete er als (fast fertig studierter) Wirtschaftswissenschaftler das Unternehmen gemeinsam mit seinem Partner aufgrund vorangegangener Erfahrung aus verschiedenen IT-Projekten und -Audits.

Heute verantwortet Jürgen bei der iQSol GmbH den Bereich Sales, PR & Marketing und treibt das IT-Security-Business gemeinsam mit seinem Team voran. iQSol ist seine zweite erfolgreiche Unternehmensgründung, denn auch am Aufbau der Antares NetlogiX Netzwerkberatung GmbH ist er schon seit Beginn im Jahr 2001 beteiligt.

iQSol GmbH
Oed 119
A - 3312 Oed

T: +43 7472 207 67
E: office@iqsol.biz

www.iqsol.biz