



## Klarheit und Nachvollziehbarkeit Das Richtige richtig tun – auch in der IT Security



„Spätestens der Verzicht oder die Reduzierung von Sicherheitsmaßnahmen erfordern klare Vereinbarungen mit dem IT Provider, um ungewollten Überraschungen vorzubeugen.“

Sascha Jäger, Director Sales & Marketing,

Unternehmensprozesse werden in Zeiten einer weltweiten Wirtschaftskrise und wirtschaftlicher Engpässe immer kritischer unter die Lupe genommen, um Investitionen und Geschäftspartnerschaften abzusichern. Mit übergreifenden (SOX, Basel2) und branchenspezifischen Regularien

wird versucht, ein Qualitätsmaß zu gewährleisten, ähnlich einem TÜV-Stempel um ein Auto in Deutschland betreiben zu dürfen. Das erfordert für die in fast allen Geschäftsprozessen nötigen und teilweise etablierten Sicherheitsmechanismen ein erhöhtes Maß an Klarheit und Nachvollziehbarkeit.

Ein vergleichbarer Bedarf an Klarheit entsteht, wenn IT Security-Investitionen eingeschränkt werden. Allerdings ist es hierbei fast immer der Fall, dass neben den Antworten auch die Fragen fehlen, d.h. die Anforderungen nicht klar formuliert sind. Insbesondere wurde dies in der Partnerschaft Geschäftsprozess/IT/IT Security innerhalb der Unternehmen in der Vergangenheit aus unserer Sicht vernachlässigt. Spätestens der Verzicht oder die Reduzierung von Sicherheitsmaßnahmen erfordern klare Vereinbarungen mit dem (internen) IT Provider, um ungewollten Überraschungen vorzubeugen.



**Integralis Deutschland GmbH**

Robert-Bürkle-Straße 3

D-85737 Ismaning

Tel.: +49(0)89.94573-0

Fax: +49(0)89.94573-199

de.info@integralis.com

www.integralis.com

## Klarheit und Nachvollziehbarkeit

### Das Richtige richtig tun – auch in der IT Security

Zusammenfassend lässt sich feststellen, dass heute mehr denn je in den Unternehmen die Forderung nach einer transparenten und wirksamen IT Security besteht.

Wie kann diese Transparenz erreicht werden? Um es einfach zu formulieren: man sollte das Richtige tun und dies sollte man dann richtig tun (Effektivität und Effizienz nach Peter F. Drucker, US-amerikanischer Ökonom) Integralis widmet dieser Thematik eine eigene Roadshow im Herbst 2009. Die Veranstaltung beschäftigt sich im ersten Teil der Frage nach dem Erreichen von Effektivität. Dazu stellen die Experten der Integralis ein Managementmodell (ISMS nach ISO 27001) vor, dass eine Entscheidungsgrundlage für den Einsatz von Sicherheitsmaßnahmen oder eben auch eine Quantifizierung der Folgen von deren Streichung bietet.

Außerdem wird vorgestellt, welche Softwaretools die effiziente Umsetzung eines solchen Managementsystems ermöglichen.

Im zweiten Teil werden Methoden und Werkzeuge vorgestellt mit denen sich die Effizienz bei den verbreitetsten IT-Sicherheitsmaßnahmen, wie z.B. Firewalls verbessern lässt.

Eine Neuheit zeigen wir auf unserer Tour durch 3 Länder auch mit unserem Solution Campus. Hier werden in einem virtuellen Unternehmensumfeld die in den Vorträgen behandelten Werkzeuge live präsentiert und im Zusammenspiel dargestellt.

# Managed Security Services – Überwachung, Alarmierung und Betriebsunterstützung



„Die im Kundennetzwerk installierte Security Service Appliance bietet die einzigartige Möglichkeit, die angebundenen Systeme zu überwachen und darüber hinaus, die Analyse von Logfiles in Echtzeit durchzuführen.“

Guido Moezer, Product Manager Support- und Managed Services

## Managed Security Services – Überwachung, Alarmierung und Betriebsunterstützung

Managed Security Services (MSS) beschäftigt sich vor allem mit der Überwachung, Alarmierung und Betriebsunterstützung von IT-Security Systemen des Kunden. MSS unterteilt sich wiederum in die Services SecureWatch (proaktiv,

Co-Managed) und die SecureManage (aktiv, Fully-Managed) und wird – damit eine qualitativ hochwertige Durchführung dieser Dienstleistungen gewährleistet ist – weltweit durch mehrere Security Operation Centern (SOC) der Integralis angeboten. Der Kunde profitiert so von einem Rund-um-die-Uhr-Service mit hochqualifizierten Sicherheitsexperten.

## Was genau bietet MSS der Integralis?

Integralis hat eine eigene weltweite, ausfallsichere Architektur aufgebaut und mit dem Integralis Security Information Service (ISIS), einem eigenen Security Information und Event Management (SIEM) und der Security Service Appliance (SSA) vorausschauende Entwicklungsarbeit geleistet. Die im Kundennetzwerk installierte SSA bietet die einzigartige Möglichkeit, die angebundenen Systeme zu überwachen und darüber hinaus, die Analyse von Logfiles (Betriebssystem und Applikation) in Echtzeit durchzuführen. Es werden täglich Hunderttausende von Log-Einträgen analysiert, ohne dass diese Datenmengen über das Netz transferiert werden müssen und somit die Datenleitungen des Kunden belasten. Die Auswertung der von den Systemen erhaltenen Daten erfolgt

direkt in der SSA, welche die verdichteten und korrelierten Daten dann zur weiteren Auswertung über eine sichere, ausfallgeschützte Verbindung in die Integralis-SOCs überträgt. Gleichzeitig dient die SSA als gesicherter Remote-Zugang zu den im Hause des Kunden betreuten Systemen. Bei Ausfall der Internetleitung oder der Firewall erfolgt der Verbindungsaufbau automatisiert über zusätzliche Dial Up-Leitungen. Diese Entwicklungsarbeit trägt entscheidend dazu bei, dass Integralis seinen Kunden den in dieser Form einzigartigen Managed Security Service weltweit anbieten kann.

## Immer ein Optimum an Sicherheit

Die in den SOC's beheimateten Sicherheitsexperten von Integralis sind rund um das Thema Sicherheit ausgebildet und zertifiziert. Dies bedingt nicht nur Trainings in Sicherheitstechnologien, Sicherheitsarchitekturen und den damit verbundenen Produkten, sondern insbesondere auch die Umsetzung von Prozessen und Richtlinien, die durch entsprechende Zertifizierungen der SOC's dokumentiert sind. Ein weltweites Team aus Sicherheitsexperten konzentriert sich ausschließlich auf den Schutz der Systeme und der Vermögenswerte der Kunden. Somit können sich Integralis Kunden darauf verlassen, immer ein Optimum an Sicherheit zu erhalten.

Die Integralis bietet ihren Kunden eine große Auswahl an Services an, die entsprechend der kundenindividuellen Geschäftsanforderungen auch angepasst werden können:

## Integralis Secure Managed Services

Integralis übernimmt die permanente (7x24) Echtzeitüberwachung sowie die Wartung und den Betrieb der überwachten Kundensysteme. Die Leistungen werden remote über gesicherte Zugänge erbracht.

Der Service umfasst im Wesentlichen:

- Die Überwachung und Alarmierung rund um die Uhr an 365 Tagen im Jahr.
- Die Überwachung der Funktionsfähigkeit der Systeme.
- Die Überprüfung der Verfügbarkeit der Systeme.
- Die Echtzeitüberwachung relevanter Systemparameter.
- Die detaillierte Auswertung und Analyse der Logdateien nach Angriffen und Abwehr von Gefahren durch verschlüsselten Zugriff auf die Systeme.
- Die Eskalation der notwendigen Aktionen auf Basis der Analyse.
- Tägliche Berichte über kritische Vorfälle und einen wöchentlichen Statusbericht mit Aufgliederung der gelogten Verbindungen nach Abweichung von der vereinbarten Policy, abrufbar über das sichere Integralis Web-Portal (ISIS Portal).
- Individuell über das Web-Portal zu erstellende Statistiken.
- Die Darstellung der Angriffe in über das Web-Portal abrufbaren Berichten.
- Die Überprüfung der Verfügbarkeit weiterer Dienste und Systeme.
- Alarmierung anhand von gemeinsam definierten Reaktionsstufen.
- Die Information über neue Veröffentlichungen zu Sicherheitslücken für die eingesetzte Security Software.
- Die Entwicklung eines Maßnahmenplans in Zusammenarbeit mit dem Kunden, um die Reaktionen je nach Grad der Gefährdung zu definieren.
- Die Umsetzung der notwendigen Aktionen, die aus der Analyse ermittelt wurden.
- Ein Systemplattform-Management, welches Konfiguration, Sicherung, Backup und Patch-Management beinhaltet.
- Ein Regelsatz-Management sowie remote Disaster Recovery.

Der Integralis SecureManage Premium Service wertet zudem, neben den rele-

vanten Betriebsparametern, alle Ereignisse der Applikations-Log-Datei aus, fasst diese korreliert zusammen und ist mit diesen gewonnenen Informationen in der Lage, nahezu alle verdächtigen Aktionen zu erkennen, um daraus eine vollständige Sicherheitsanalyse abzuleiten. Mit der Echtzeitanalyse von Sicherheitsvorfällen im Netzwerk rund um die Uhr können selbst äußerst komplexe Hacker-Angriffe aufgespürt werden. Die potenziellen Angriffe werden entsprechend ihrem Gefährdungspotenzial priorisiert und in den SOCs manuell qualifiziert. Darauf werden die mit dem Kunden vereinbarten Gegenmaßnahmen eingeleitet (Incident und Change Management).

#### **Logfile Analyse**

Im Bereich der Logfile-Analyse überwacht und analysiert Integralis die Protokolldateien der definierten Systeme. Die Protokolldateien werden hierbei für Sicherheits- und Verfügbarkeits-Zwecke ausgewertet. So können nicht nur Missbräuche erkannt und eskaliert werden, auch lassen sich unter anderem durch plötzlich verändertes Log-Verhalten z.B. nichtautorisierte Änderungen an Sicherheits-Applikationen oder Viren- und Wurmausbrüche aufdecken (statistische Analysen). Im Anschluss werden die Informationen aufbereitet und an das Incident Management weitergegeben. Weiterhin werden durch die Protokoll-Analyse wichtige Informationen über die Effektivität der Policies, die Qualität der Security-Anwendungen, die Bedrohungsstatistiken und das Missbrauchsverhalten sowie allgemeine KPIs über Sicherheitsparameter für Reports gewonnen.

### **Incident Management**

Beim Incident Management werden kritische Incidents an Hand einer Protokolldaten-Analyse gemeldet. Das Incident Management beinhaltet die Bearbeitung von Anfragen und Störungen aller Art, mit dem Ziel der schnellstmöglichen Wiederherstellung der Service Leistung und Minimierung der Beeinträchtigung von Geschäftsprozessen.

### **Change Management**

Beim Change Verfahren werden zusammen mit dem Kunden im Vorfeld folgende Punkte definiert:

- Regelbasisänderung aufgrund kritischer Incidents/Sicherheitsvorfälle
- Regelbasisänderungen, eingereicht durch Kunden
- Regelbasisänderungen, auf Empfehlung von Integralis

Bei allen Vorgängen wird eine automatische Dokumentation in ISIS (Integralis Security Information Service) vorgenommen. Alle Aktivitäten lassen sich durch Reports visualisieren.

Weitere Informationen gibt es unter [www.integralis.com](http://www.integralis.com)

# Dem Täter auf der Spur – Forensische Analysen



„Es empfiehlt sich daher, im Vorfeld Schutzmaßnahmen zu etablieren, um gegen interne und externe Vorfälle gerüstet zu sein.“

Andreas Bröhl, Business Development Manager Audits & Assessments, CISSP, PCI QSA Auditor

## Wie kann das passieren?

Angreifer nutzen neben dem klassischen Einfallstor über das Internet oft auch Hintertüren, wie unzureichend geschützte WLAN- und RAS-Zugänge. Häufig sind aber auch interne Vorfälle durch Mitarbeiter des Unternehmens, externe Dienstleister, oder Wartungsfirmen die Ursache.

Fest steht: Die Vielfalt interner Sicherheitsvorfälle ist groß. Bekannte Szenarien sind Infektionen mit Viren, Trojanern, Würmern oder Spyware, die Installation von Rootkits, die Ablage von illegalen bzw. pornographischen Daten, Verstöße gegen interne Policies, z.B.

eine illegale Email- und Internetnutzung, illegales Filesharing, Sabotage durch frustrierte Mitarbeiter, der Diebstahl von vertraulichen Informationen sowohl von Mitarbeitern als auch Wettbewerbern sowie jegliche Form von internem und externem Betrug.

## Was können Sie tun?

Es empfiehlt sich daher, im Vorfeld Schutzmaßnahmen zu etablieren, um gegen derartige Vorfälle gerüstet zu sein. Es sollte zu allererst sichergestellt sein, dass ein effektives Incident Management etabliert wurde. Ohne einen fest definierten Prozess werden Sicherheitsvorfälle oft inkonsistent und nicht beweissichernd bearbeitet. Bei guter Planung und der richtigen Beratung im Vorfeld sind die Verantwortlichkeiten hingegen klar definiert und es werden die richtigen Schritte durchgeführt, um alle potentiellen Beweismittel ohne Veränderung sicherzustellen.

So sollten Sie immer gewährleisten:

- Dass die richtigen Ansprechpartner bei einem Sicherheitsvorfall informiert werden. Es ist empfehlenswert durch regelmäßige Sensibilisierungsmaßnahmen, z.B. Security-Awareness-Trainings, diese Vorgehensweisen aufzufrischen, damit sie auch wirklich von den Mitarbeitern gelebt werden. Die Sensibilisierung der Mitarbeiter ist ein wichtiger Faktor zur Vermeidung von Sicherheitsvorfällen.
- Dass bei der Durchführung der technischen Untersuchung jeder einzelne Aspekt der Prüfung sorgfältig und konsistent durchgeführt wird. Beispielsweise ist zu Beginn einer Untersuchung nicht klar, ob ein trivialer Verstoß gegen Email-Richtlinien sich nicht später als symptomatisch für ein ernsthaftes Betrugsvergehen darstellt. Falls diese Beweise dann nicht sorgfältig gesichert wurden, kann das Betrugsvergehen später eventuell nicht mehr nachgewiesen werden.

Im Rahmen der Analyse eines Sicherheitsvorfalles sind weitere Aspekte zu beachten:

- Für die Beweissicherung auf Computersystemen gibt es spezielles Hardware-Equipment sowie viele Software-Tools (z.B. Encase oder Access Data FTK). Jede Aktion die ein Beweismittel (z.B. eine Festplatte) verändert, kann dieses Beweismittel rechtlich unzulässig werden lassen. Mit entsprechender Schreibschutzhardware kann ein Schreiben auf Festplatten und andere Datenträger verhindert werden. Allgemein ist empfohlen ein Sektor-Abbild (Image) von der Festplatte zu erstellen. Bei Kriminalverfahren werden in der Regel zwei Images erstellt, eines zur eigentlichen Analyse und eines als versiegelte und gesicherte Masterkopie.

- Dabei dürfen keine Beweise zerstört werden, die aus Sicht von anderen Abteilungen des Unternehmens Relevanz haben könnten. Idealerweise bildet man ein Projektteam aus verschiedenen Abteilungen, z.B. HR, IT, Werksschutz, Rechtsabteilung und Spezialisten für Business-Anwendungen und Systeme. Nach Beendigung der Untersuchungen empfiehlt es sich, die gewonnen Erkenntnisse auszuwerten, um mögliche Schutzmaßnahmen zur Vermeidung derartiger Vorfälle zu identifizieren. Dies sollte im Rahmen regelmäßiger Management-Reviews und Trend-Analysen geschehen.
- Schließlich ist die rechtliche Grundlage bei allen forensischen Tätigkeiten zu beachten. Die gültigen Vorschriften sind abhängig vom Ort der Untersuchungen. Jedes Land hat seine eigenen Gesetze, die beachtet werden müssen und Einfluss auf den Ablauf einer Analyse haben. In Deutschland ist dies u. a. das Bundesdatenschutzgesetz. Neben der Beachtung der örtlichen Gesetze ist auch immer eine ausdrückliche Genehmigung zur Durchführung der Untersuchungen notwendig. Ist in strafrechtlichen Analysen in der Regel eine enge Kooperation mit den Polizeibehörden erforderlich, sollte bei einer Untersuchung im Auftrag eines Unternehmens unbedingt darauf geachtet werden, dass der Auftrag von einer autorisierten Person erfolgt. Dies ist normalerweise die Geschäftsleitung des Unternehmens in dem die Prüfung durchgeführt wird.

#### **Lassen Sie sich helfen!**

Natürlich ist es aber auch immer ratsam, sich einen externen Experten ins Haus zu holen. Mit den Services „Network Forensics“ bzw. „Computer Forensics“ bietet Integralis eine umfassende Analyse der betroffenen Systeme um kompromittierte Daten oder zusätzlich betroffene Systeme zu ermitteln. Zudem

sucht Integralis nach dem Einstiegspunkt des Angreifers und identifiziert so die Schwachstellen in Ihrem Netzwerk. Am Ende wird schließlich ein umfassender Bericht erstellt, der das Ausmaß der Kompromittierung beschreibt sowie Empfehlungen zur Beseitigung der gefundenen Schwachstellen sowie zur Wiederherstellung Ihrer Systeme beinhaltet.

Die Spezialisten von Integralis helfen Ihnen dabei:

- Daten forensisch einwandfrei zu sichern,
- Daten nach Beweisen und Spuren zu untersuchen,
- Daten wiederherzustellen und nach Indizien zu suchen,
- Ihr eigenes Vorgehen einwandfrei und lückenlos zu dokumentieren,
- Schwachstellen zu identifizieren,
- Sicherheitsvorfälle möglichst lückenlos zu erfassen sowie
- die Erkenntnisse in verwertbaren und verständlichen Berichten zusammen zu fassen.

Dabei führen sie Analysen von Festplatten, der physischen Speicherabilder (RAM), der USB-Geräte und Speicherkarten oder der Log-Files von Netzwerkkomponenten durch.

Weitere Informationen gibt es unter [www.integralis.com](http://www.integralis.com)

# Outsourcing – Wie kontrolliert man eigentlich die Dienstleister?



„Gerade in Zeiten, in denen es immer häufiger zu unzuverlässigem Umgang mit Daten kommt, reicht Gutgläubigkeit nicht mehr aus.“

Uwe Maurer, Business Development Manager Security Operations, CISSP

## Outsourcing – Wer kontrolliert eigentlich die Dienstleister?

Der Trend zum Outsourcing zeichnete sich bereits im vergangenen Jahr ab, doch die aktuelle wirtschaftliche Lage zwingt weitere Unternehmen, über Einsparungen in allen Bereichen nachzudenken.

Vor allem in der IT und IT-Security wird der Rotstift ange-setzt. Auch, weil viele Infrastrukturprojekte den schnellen Nutzen oder sofortige Einsparungen kaum nachweisen können. Selbst bei Projekten, deren Rentabilität oder strategischer Nutzen offensichtlich sind, wird gespart. Viele Unternehmen

entschließen sich unter diesen Bedingungen, die Kapitalausgaben zugunsten von Betriebsausgaben zu reduzieren. Das geht zum Beispiel, indem wichtige Rationalisierungen verschoben werden oder Aufgaben komplett über einen Dienstleister abgewickelt und als Betriebsausgaben verrechnet werden.

## Kontrolle externer Dienstleister wird immer wichtiger

Die Aufgaben für die Dienstleister nehmen daher in Zeiten der finanziellen Krise mit weniger Budget eher zu. Für immer mehr Unternehmen heißt das, sie müssen den Dienstleistern vertrauen und sind auf eine zuverlässige Arbeit dieser angewiesen. Denn sie erwarten hohe Effizienz sowie Fehlerfreiheit und gehen davon aus, dass die eigenen Daten in sicheren Händen sind. Doch gerade in Zeiten, in denen es immer häufiger zu unzuverlässigem Umgang mit Daten kommt, reicht Gutgläubigkeit nicht mehr aus. Es wird daher immer wichtiger, die Dienstleister zu kontrollieren. Die meis-

ten Compliance-Regularien raten zu einer laufenden Verhaltenskontrolle der Externen.

Auch, weil in letzter Zeit immer wieder Fälle bekannt wurden, in denen Dienstleister tatsächlich Schadensverursacher waren oder bei einem Schaden sofort verdächtigt wurden. Eine später verwertbare Erfassung der sensiblen Aktivitäten wäre hier sicher sinnvoll gewesen.

## Wie können Dienstleister kontrolliert werden?

Bei der Kontrolle von Dienstleistern geht es nicht nur um die notwendige laufende Verhaltenskontrolle, sondern auch um Erfolgskontrolle. Diese orientiert sich an den zugesagten Leistungen. So sollte bei Outsourcing und Betriebsunterstützung beispielsweise noch die Erbringung der folgenden Aufgaben überwacht werden:

Ordnungsgemäßes Systemmanagement mit der Gewährleistung von Funktions- und Sicherheitsstandards:

- Vermeidung und Beseitigung von kritischen Schwachstellen
- Korrektes, effizientes und voll dokumentiertes Change-Management
- Überwachung der Funktion und Sicherheit der Systeme sowie schnelles kompetentes Fehlermanagement
- Laufende Reviews und Verbesserungen der Systemkonfigurationen
- Vorbereitung auf Audits durch regelmäßiges und vollständiges Reporting

Zusätzlich muss selbstverständlich der

Umgang des Dienstleisters mit sensiblen Daten kontrolliert werden. Genau genommen bedeutet das:

- Einhaltung der gesetzlich empfohlenen und vereinbarten Verfahrensweisen beim Datenhandling
- Einhaltung der Sicherheitsrichtlinien beim (Fern-) Zugriff und bei der Benutzung der Einrichtungen
- Beschränkung auf die Arbeit im vereinbarten Bereich
- Beschränkung der eigenen Privilegien auf das minimal Erforderliche

Letztendlich dürfen Unternehmen vom Dienstleister eine ausreichende Kompetenz, Prozesseffizienz und Fehlerfreiheit erwarten.

## Sicherheit für webbasierte ERP-/CRM-Portale – Neue Möglichkeiten aber auch neue Herausforderungen



### Sicherheit für webbasierte ERP-/CRM-Portale – Neue Möglichkeiten aber auch neue Herausforderungen

Die Verfügbarkeit und Sicherheit von ERP- und CRM-Portalen wie SAP Enterprise Portal oder auch Collaboration-Anwendungen wie Microsoft SharePoint sind jederzeit (24/7) sicherzustellen, um geschäftskritische Ausfälle und nachfolgende Probleme zu verhindern. Aus diesem Grund müssen die zentralen Anwendungen in den Bereichen Collaboration, Customer Relationship Management (CRM), Enterprise Resource

Planning (ERP) und Supply-Chain permanent steigenden Sicherheits-Anforderungen entsprechen, denn die Erfahrungen aus klassischen E-Business Plattformen für Webshops zeigen, dass gezielte Angriffsversuche auf Webanwendungen sehr verbreitet sind und bei nahezu jedem Webserver Spuren davon in den Weblogs zu finden sind. Fast alle Webserver weisen entsprechende Schwachstellen auf und Hacker haben dies längst erkannt. Über 90% der Angriffe finden laut dem Marktforschungsinstitut Gartner mittlerweile auf Anwendungsebene statt. Klassische Netzwerk-Firewalls bieten für die Angriffe jedoch nur einen geringen Schutz, da sie den Zugriff von außen auf die internen Webserver grundsätzlich zulassen müssen.

E-Business- oder Portal-Anwendungen sind stark mit den internen Systemen (Daten- und Anwendungsservern, Datenbanken, etc.) verbunden – die angebotenen Daten müssen aktuell

sein und damit laufend mit den internen Systemen aktualisiert werden. Gelingt es einem Angreifer, die Webanwendung zu komprimieren, hat er Zugang zu den inneren, sensiblen Systemen.

### Welche Angriffe auf Web-Portale gibt es und wie sehen Sicherheitsrisiken bei webbasierten ERP-/CRM-Portalen aus?

Für Web-Angriffe sind keine Spezialtools erforderlich, ein Browser reicht in allen Fällen aus. Diese Angriffe erfolgen über browserbasierte Benutzeranfragen (Requests) direkt auf die Webanwendung und deren Daten.

Selbst für die einfachsten Angriffe sind Schwachstellen auf bekannten Webauftritten zu finden: Force-Full-Browsing, Manipulation von Hidden Fields, Backdoors, Cross Site Scripting, Parameter-Tampering, Buffer-Overflow, Cookie-Poisoning, SQL-Injection, um nur einige zu nennen.

Ein webbasiertes ERP-/CRM-Portal ist zudem eine komplexe Webanwendung mit verschiedenen Schnittstellen und wird oft als Mitarbeiter-Portal für interne Anwendungen genutzt. Jedoch werden immer häufiger auch externe Zugriffe auf zentrale Geschäftsprozesse von unsicheren Netzen wie dem Internet aus für Kunden, Geschäftspartner, Lieferanten und Dienstleister über das Portal realisiert – die Erreichbarkeit muss daher jederzeit und weltweit gewährleistet sein für:

- Beziehungen zu Kunden und Lieferanten (CRM)
- Produktmanagement, Geschäftsmöglichkeiten und Dienstleistungen (PLM)
- geschäftliche Transaktionen, Logistik- und Liefermanagement (SCM – Supply Chain Management)
- Personalabteilung, Personalplanungsmanagement (HRMS – Human Resource Management Systems)

„Die Ziele eines Unternehmens, das seinen Kunden und Partnern einen Zugang zu webbasierten Portal-Anwendungen bietet, sollten in der Gewährleistung der Sicherheit, aber auch der Verfügbarkeit und der Performance dieses Portals bestehen.“

Von Norman Wenk, Senior Consultant Business Development Secure Application Delivery

### Wie kann ein webbasiertes ERP-/CRM-Portal geschützt werden?

Zur vorbeugenden Abwehr von Angriffen auf Anwendungsebene kann man sich daher nicht nur ausschließlich auf die Sicherheit des Codes verlassen, sondern muss eine Sicherheitskomponente davor schalten. Es ist daher notwendig, eine Firewall auf Anwendungsebene einzurichten, die den Datenfluss analysiert und filtert. Dabei bildet der Regelsatz als zentrales Schutzelement die für die Anwendung erforderlichen Anfragen ab (White-List-Ansatz). Alles andere wird ausgefiltert und löst gegebenenfalls Alarme aus.

Die Ziele eines Unternehmens, das seinen Kunden und Partnern einen Zugang zu webbasierten Portal-Anwendungen bietet, sollten in der Gewährleistung der Sicherheit, aber auch der Verfügbarkeit und der Performance dieses Portals bestehen. Eine geeignete Umgebung für das SAP-Portal muss aus diesem Grund mindestens die folgenden Funktionen erfüllen:

- Performance durch Serverentlastung (SSL-Terminierung/Offloading, Caching, TCP-Optimierung, Compression)
- Verfügbarkeitssicherung durch Load-Balancer und geeignete Serviceüberwachung
- Reverse Proxies, um die Zugriffe umzuschreiben und die Verbindungen zu terminieren
- Ein Intrusion-Prevention-System zum Schutz gegen Denial-Of-Service-Angriffe und als Schutz gegen Denial-Of-Service-Angriffe auf Anwendungsebene
- Eine Web Application Firewall (WAF), um nur die erwünschten Zugriffe durchzulassen
- User-Authentifizierung gegenüber Local Directories bzw. Mechanismen und Lösungen für starke Authentifizierung und nachgelagertem Single-Sign-On.

Alle diese Komponenten sind in den modernen Systemen zur Portalsecurity, sogenannten Application Delivery Controllern (ADC) konsolidiert. Die genauen Vorteile für Ihr Unternehmen erfahren Sie bei einem Gespräch mit der Integralis.

Durch die Verringerung der notwendigen Server und Devices werden Ihre Betriebskosten maßgeblich reduziert. Eine weitere Reduktion ergibt sich durch hochentwickelte Appliances, die alle notwendigen Funktionen eines ADCs inklusive WAF integrieren. Die Betriebskosten von Appliances und Netzkomponenten können mit etwa 10-15% derer von Serversystemen geschätzt werden. Diese Systeme sind in der Lage, alle Anforderungen eines Unternehmens zu erfüllen und bilden eine optimale Grundlage für den Aufbau einer generischen Plattform für das ERP-/CRM-Portal, mit der die nachhaltige Sicherheit der Anwendungen gewährleistet werden kann.