

Zentrale Managed Security Services

## Angemessene Internet-Sicherheit für die Kölner Druckerei Moeker Merkur

Dr. Kurt Brand, Pallas GmbH  
Stephan Sachweh, Pallas GmbH  
Friedhelm Spohr, Moeker Merkur GmbH

Sicherheit ist für das bereits seit 1844 in Köln ansässige Druck- und Medienunternehmen Moeker Merkur GmbH schon immer ein Leistungsanspruch gewesen. Sicherheit heißt termingerechte Abwicklung, und das ist ohne Internet-Sicherheit heutzutage nicht mehr möglich. Einem typischen Mittelständler fehlt aber das Know-how, die Internet-Sicherheit auf einem gleichbleibend guten Stand zu halten. Moeker Merkur mietet deshalb diese Sicherheit bei der Pallas GmbH. Die Pallas-Lösung kommt ohne Vor-Ort-Installation aus und bietet Schutzbausteine je nach Bedarf und zur festen monatlichen Miete. Sie ist deshalb einfach, leistungsfähig und erschwinglich.

Bei Moeker Merkur nutzen etwa 30 Mitarbeiter das Internet, teilweise von Windows-Arbeitsplätzen aus, teilweise auch von Mac-Rechnern. Dabei sind Email und Web die Standardapplikationen. Insbesondere die Kommunikation über Email ist bereits zur unternehmenskritischen Applikation geworden, da Angebote, Bestellungen und Layoutdaten auf diese Weise schnell und direkt ausgetauscht und weiterverarbeitet werden können.

### Bedarf oder Auslöser?

Ein Bedarf nach mehr Internet-Sicherheit lässt sich letztlich bei allen Unternehmen schnell ausmachen. Da es keine hundertprozentige Sicherheit gibt, ist Sicherheit immer relativ zu sehen. Wenn man verstehen will, wie angemessene Internet-Sicherheit entsteht, lohnt es sich deshalb mehr, nach den auslösenden Faktoren für einen Zuwachs an Sicherheit zu suchen, als nach dem Bedarf. Bei Moeker Merkur waren die folgenden Auslöser entscheidend:

- Der Datenaustausch enthält zunehmend unternehmenskritische Daten.
- Das Vertrauen in die Sicherheitskompetenz des vorhandenen IT-Dienstleisters hatte deutlich abgenommen. Hier ist zur Ehrenrettung zu sagen, dass ein IT-Allrounder ohne

Spezialisierung nicht dauerhaft angemessen auf die dynamischen Internet-Bedrohungen reagieren kann.

- Die Geschäftsführung von Moeker Merkur will verantwortungsvoll mit IT-Risiken umgehen und kein Privathaftungsrisiko eingehen (§ 43 GmbH-Gesetz und § 266 StGB).

### Die Schwachstellenanalyse

Es macht keinen Sinn, IT-Sicherheit punktuell anzugehen. Eine mehrstufige, redundante Firewall bringt für sich allein keinen guten Schutz, wenn der Virenschutz vernachlässigt wird. Deshalb ist es prinzipiell wichtig, den Verbesserungsprozess zumindest mit einer kurzen Schwachstellenanalyse zu beginnen. Diese konzentriert sich auf Kernbedrohungen und kritische Systeme und hält dadurch die Kosten sehr niedrig.

Trotzdem wird hier im Rahmen einer Begehung die gesamte IT-Infrastruktur überprüft. So können in einem Bericht die wirklich

kritischen Risiken nebst Verbesserungsvorschlägen festgehalten werden. Der Bericht ist auch gleichzeitig Sicherheitsrichtlinie für weitere Maßnahmen.

Die Schwachstellenanalyse der IT-Infrastruktur bei Moeker Merkur bestätigte tatsächlich, dass der frühere IT-Dienstleister ein Sicherheitsrisiko hinterlassen hatte. Ein Zugang vom Internet her auf das interne Netzwerk (Remote-Zugang für Fernwartung) war sicherheitskritisch angelegt worden. Im Prinzip ist ein Remote-Zugang sinnvoll, weil er einem Dienstleister ermöglicht, schnell und kostengünstig Unterstützungsleistungen zu erbringen. Dieser Zugang muss aber gut geschützt werden, andernfalls stellt er eine offene Tür ins Unternehmensnetz dar.

Durch eine bessere Konfiguration konnte auch die folgende Schwachstelle beseitigt werden. Der Mailserver war nämlich so eingerichtet, dass er seinen Software-Stand jedem Externen bekannt machte. Ein Angreifer weiß dann, welche Angriffsflächen der Mailserver bietet, problematisch insbesondere, wenn der Server sich nicht auf dem neuesten Stand befindet

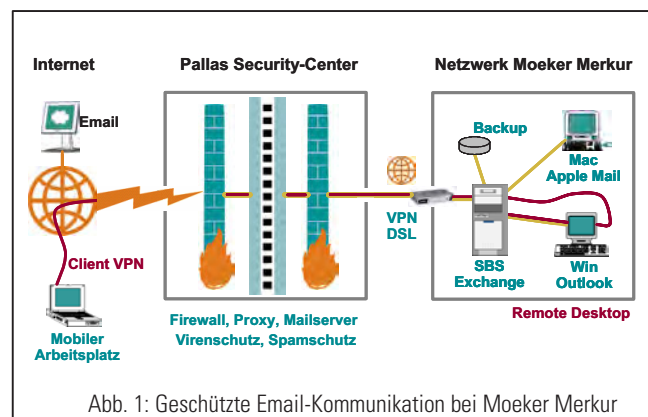


Abb. 1: Geschützte Email-Kommunikation bei Moeker Merkur

(nicht gepatcht wurde). Es handelt sich hier um eine typische Schwachstelle, wie sie sehr häufig vorkommt. Sie ist letztlich darauf zurückzuführen, dass der Administrator operative Aufgaben zu erfüllen hat, also den Mailserver möglichst "geräuschlos" im Betrieb halten muss. Konfigurationsänderungen, die präventiven Charakter haben, können aber das operative Geschäft stören, falls überhaupt ein Bewusstsein für ihre Notwendigkeit vorhanden ist.

Durch stichprobenartige Überprüfung stellte sich außerdem heraus, dass der Virenschutz auf den einzelnen Arbeitsplätzen uneinheitlich war. Dies ist eine typische Mangelerscheinung einer dezentral gepflegten Internet-Sicherheit.

### Was ist zu tun?

Jedes Unternehmen sollte heute mindestens über die folgenden Internet-Sicherheitsmaßnahmen verfügen:

- Firewall am Übergang zwischen Unternehmensnetz und Internet, also am Gateway; möglichst mehrstufig, also nicht nur Paketfilter, sondern auch Sicherheits-Proxy (Application Level Gateway), so dass der direkte Datenstrom zwischen Quelle und Ziel unterbrochen wird. Das BSI (Bundesamt für Sicherheit in der Informationstechnik) empfiehlt fast ausnahmslos einen solchen mehrstufigen Aufbau.
- Virens Scanner am Gateway, mindestens täglich aufgefrischt (besser noch öfter, bei Pallas alle 5 Minuten)
- Spamfilter sofern nötig gegen Effizienzverlust
- Immer neueste Versionen von System- und Sicherheitssoftware (d.h. patchen)
- Desktop Virenschutz auf allen Systemen (sonst z.B. Virengefahr über USB)
- Zusätzlicher Schutz auf bestimmten Systemen: Desktop Firewall für mobil eingesetzte Rechner, Client VPN (Virtual Private Network) für Systeme, die von draußen auf das Firmennetz zugreifen müssen (z.B. für Mail)

Zunehmend setzt sich die Erkenntnis durch, dass Sicherheitsmaßnahmen integriert erfolgen sollen, weil sie dann aufeinander abgestimmt werden können und keine teure Insellösung entsteht. Bei Moeker Merkur werden alle diese Anforderungen durch die mietweise Nutzung der im Security-Center von Pallas vorgehaltenen Sicherheitsbausteine erfüllt. Durch einen VPN-Anschluss des Firmennetzwerkes an das Security-Center wird sichergestellt, dass jeder Zugriff auf das Firmennetz nur über das Security-Center erfolgen kann. Moeker Merkur wird sozusagen hinter dem Security-Center "versteckt", siehe Abbildung 1. Die Schutzfunktionen lassen sich jederzeit flexibel an den Bedarf anpassen, es sind keine Investitionen bei Moeker Merkur erforderlich, und durch den zentralen Betrieb bei Pallas - Experten betreuen die Systeme rund um die Uhr - wird die Sicherheit eines professionellen Rechenzentrums erreicht. Moeker Merkur erhält regelmäßige Reports über den aktuellen Internet-Verkehr und die Sicherheitsaktivitäten.

Solche Managed Security Services werden von Sicherheitsexperten immer wieder empfohlen, sie sind hier auch unter Kostengesichtspunkten besonders vorteilhaft, da eine zentral vorhandene Infrastruktur mitgenutzt wird. Insgesamt ist der hier vorgestellte Service für die Internet-Sicherheit mittelstandtauglich, d.h. betriebswirtschaftlich sinnvoll und technisch angemessen,

- weil er einfach ist, nämlich ohne Installation im Hause auskommt,
- weil er leistungsfähig ist durch sein Baukastenprinzip und
- weil er erschwinglich ist durch eine feste, niedrige Miete pro Arbeitsplatz.

Mit dem Security Service der Pallas GmbH hat Moeker Merkur jetzt eine Bausteinelösung, die mit dem Bedarf wachsen kann und es dem Unternehmen erlaubt, im Kerngeschäft seinem Leistungsanspruch Qualität - Flexibilität - Sicherheit - Zuverlässigkeit weiter gerecht zu werden.

### Erfahrung und Innovation

Moeker Merkur steht seit mehr als 160 Jahren für hochwertige und wirtschaftlich hergestellte Druck- und Medienezeugnisse. Moeker Merkur übernimmt die komplette Abwicklung von der Layouterstellung, über Satz, Scannen, Drucken auch auf großformatigen Druckmaschinen rund um die Uhr, Verarbeiten bis hin zum Versand. Zahlreiche Dienstleistungen im Bereich der Neuen Medien runden das Leistungsspektrum ab.

### Friedhelm Spohr

Geschäftsführer Moeker Merkur GmbH

### Weitere Informationen

Friedhelm Spohr  
Moeker Merkur GmbH  
Niehler Gürtel 102  
50733 Köln  
Tel: 0221-74908-0  
Fax: 0221-74908-18  
Spohr@moeker-merkur.de  
www.moeker-merkur.de

### Internet-Sicherheit einfach mieten

Die Pallas GmbH sorgt für integrierte Internet-Sicherheit zur festen Miete, angepasst an den konkreten Schutzbedarf und ohne Bindung an Investitionen. Pallas betreibt abgesicherte Internet-Server und Applikationen und berät bei der Netzwerksicherheit. Pallas hat den ASP Award gewonnen und wurde durch die Landesinitiative "secure-it.nrw" ausgezeichnet.

### Dr. Kurt Brand

Geschäftsführer Pallas GmbH

### Stephan Sachweh

Technischer Leiter Pallas GmbH

### Weitere Informationen

Dr. Kurt Brand  
Pallas GmbH  
Hermülheimer Straße 10  
50321 Brühl  
Tel: 02232-1896-0  
Fax: 02232-1896-29  
Kurt.Brand@pallas.de  
www.pallas.de