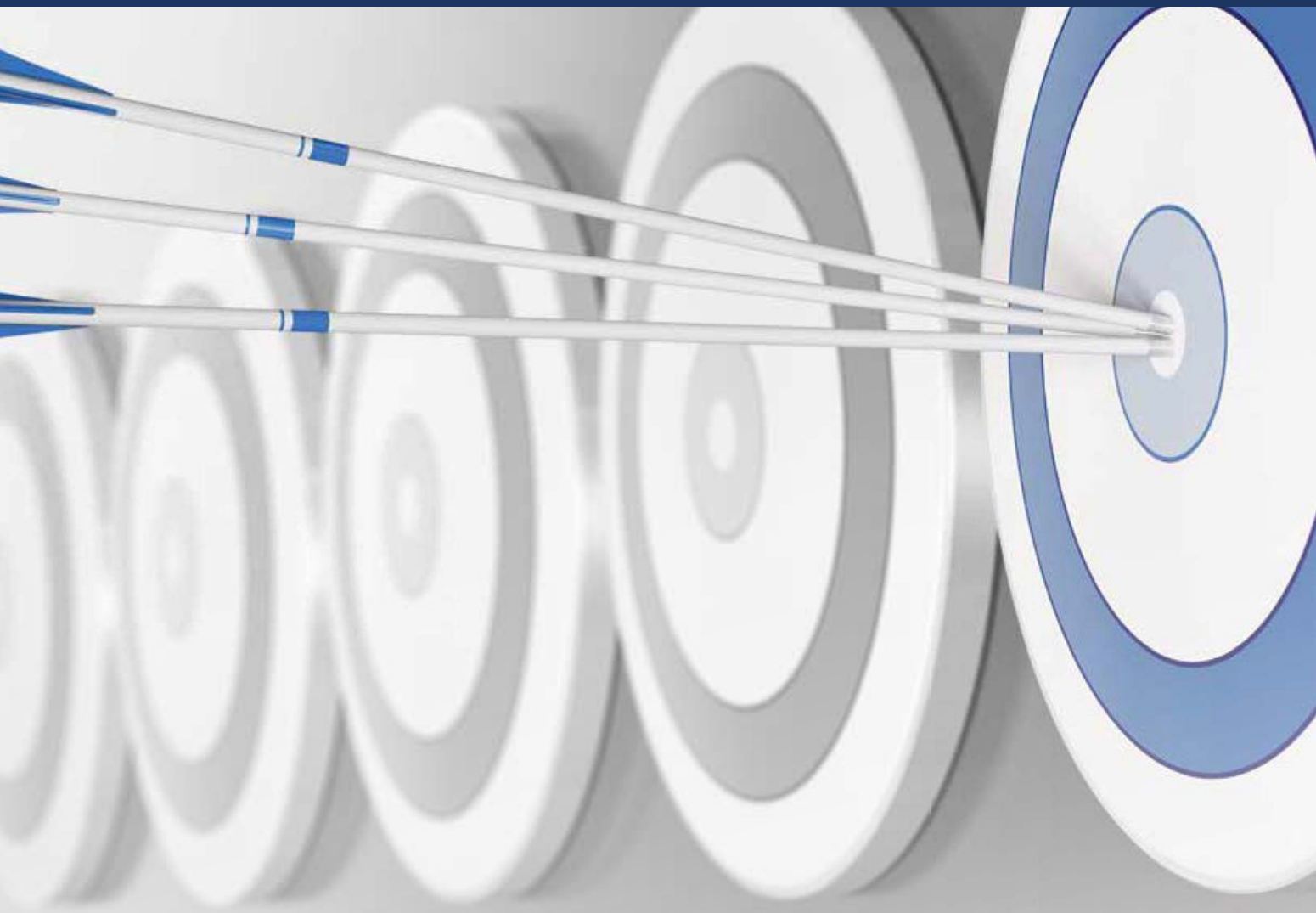
IT-SICHERHEIT

Fachmagazin für Informationssicherheit und Datenschutz

Verlagsbeilage
2|2017



UNTERNEHMEN IM VISIER

Neue IT-Security-Projekte aus der Praxis

DIE THEMEN: Netzwerksicherheit // Anomalieerkennung // Sicherheitskonzepte // Datenträgervernichtung // Datensicherheit // Web Application Security // Firewalls // Verschlüsselung // Data Leak Prevention // Viren-/Malwareschutz

DATAKONTEXT

www.itsicherheit-online.com

49187

Auch online verfügbar

Selbstverständlich können Sie die aktuelle Ausgabe unseres Sonderhefts **IT-SICHERHEIT Best Practice** auch einfach und bequem online lesen – egal, ob am PC oder via Smartphone. Probieren Sie es aus ...

www.itsicherheit-online.com/branchenguide

Mit dem E-Paper zu unserem Branchenbuch IT-Sicherheit 2017 geben wir Ihnen einen umfassenden Überblick rund um die verschiedenen Aspekte der IT-Sicherheit. Wir zeigen auf, wo überall Gefahren für Ihre Unternehmens-IT lauern, und erleichtern Ihnen die Suche nach den passenden Produkt-Anbietern bzw. Dienstleistern, die Ihnen als Experten mit Rat und Tat zur Seite stehen.

www.itsicherheit-online.com/branchenguide

Impressum

IT-SICHERHEIT
Fachmagazin für Informationssicherheit und Datenschutz
Sonderausgabe: IT-SICHERHEIT Best Practice

Verlag:
DATAKONTEXT GmbH
Augustinusstraße 9d, 50226 Frechen

Vertrieb
Jürgen Weiß
Tel.: 0 22 34/98 94 9-71
Fax: 0 22 34/98 94 9-32

www.datakontext.com
fachverlag@datakontext.com

Chefredaktion:
Jan von Knop
knop@datakontext.com

Stellvertretender Chefredakteur:
Stefan Mutschler
mutschler@datakontext.com

Redaktion:
Faatin Hegazi
hegazi@datakontext.com

Thomas Reinhard-Rief
reinhard@datakontext.com

Herausgeber:
† Bernd Hentschel

Layout:
Britta Happel
happel@datakontext.com

Anzeigen- & Objektleiter:
Thomas Reinhard-Rief
reinhard@datakontext.com

Abonnement:
Jahresabonnement € 85,-
(für Studenten, RDV-Abonnenten und GDD-Mitglieder: € 50,-)
Einzelheft € 15,- zzgl. Versandkosten
Erscheinungsweise: sechs Ausgaben

Satz: Britta Happel, DATAKONTEXT
Druck: AZ Druck und Datentechnik GmbH, Kempten

Titelbild: © Olivier Le Moal/fotolia.com
Fotos: fotolia.com, Firmenbilder
2. Jahrgang 2017 · ISSN: 1868-5757

Liebe Leserinnen und Leser,

auch das vergangene Jahr hat wieder einmal gezeigt, dass Unternehmen und Behörden gleichermaßen einen hohen Aufwand betreiben müssen, um ihr Know-how oder sensible (Kunden-)Daten vor den Zugriffen Dritter zu schützen. Ob es sich bei den potenziellen Angreifern dabei nun um selbstdarstellungssüchtige Hacker, terroristische Gruppierungen oder politisch motivierte Geheimdienste handelt, ist zunächst zweitrangig. Wichtiger festzuhalten ist auch Anfang 2017 eher: Die Angriffe auf Unternehmensnetzwerke oder kritische Infrastrukturen sind technisch immer ausgefeilter und werden immer zielgerichteter ausgeführt.

IT-Sicherheit fristet aufgrund unzähliger Vorfälle der vergangenen Jahre zum Glück längst kein Schattendasein mehr. Stattdessen avanciert das Thema immer mehr – und das auch zu Recht – zu einem wichtigen Managementthema, dem viel Bedeutung beigemessen wird. Doch wo fängt man bei der IT-Sicherheit an? Wie gewichtet man Risiken? Und wie soll man sich der schier endlosen Flut an Sicherheitslücken stellen?

Hilfreich ist an dieser Stelle oft ein Blick auf das, was andere machen. Anders, als in der Schule, ist beim Thema Sicherheit abgucken durchaus erlaubt und auch sinnvoll. Denn im Kampf um die Hoheit seiner Daten ist man keinesfalls auf sich allein gestellt. Es gibt viele Leidesgenossen, denen ebenfalls sehr daran gelegen ist, ihre Informationen unter Verschluss zu halten. Ein Erfahrungsaustausch untereinander kann da sehr hilfreich sein, um zu erkennen, welche Sicherheitsvorkehrungen sich in der Praxis bewährt haben und erfolgsversprechend sind.

Ich hoffe, dass Sie aus der neuen Ausgabe unseres Sonderhefts IT-SICHERHEIT Best Practice neue Anregungen und einen fachlichen Mehrwert für die Umsetzung Ihrer eigenen Security-Projekte mitnehmen können und wünsche in diesem Sinne viel Spaß beim Lesen.

Mit freundlichen Grüßen

Thomas Reinhard-Rief
Objektleiter IT-SICHERHEIT

Verkehrsknotenpunkt Internet: Deutsche Bahn vertraut auf ESET Gateway Security

PRODUKT

ESET Gateway Security

KUNDE

Deutsche Bahn Konzern, Frankfurt am Main

BRANCHE

Transport & Logistik

FACHHÄNDLER

arxes-tolina GmbH, Dresden

Täglich setzen 5,5 Millionen Bundesbürger auf die Deutsche Bahn (DB). Rund 70.000 Nutzer haben Zugang zu den IT-Services der Bahn und gleichzeitig zum Internet, was das Intranet potentiell anfällig für externe Angriffe macht. Seit September 2014 sorgt die ESET Gateway Security über einen Zeitraum von fünf Jahren dafür, dass jeder Bahn-Endanwender sicher auf das Internet zugreifen kann.

Deutsche Bahn AG

Ob im Nah- oder Fernverkehr, als Urlauber oder Pendler: Die Deutsche Bahn ist die ökologische Alternative zu Auto und Flugzeug. Damit der Regelbetrieb und die Netzwerksicherheit am Übergabepunkt des Bahn-Intranets zum Internet zu jedem Zeitpunkt gewährleistet ist, suchte die DB Systel GmbH, der Anbieter von Informations- und Telekommunikationsdiensten der Deutschen Bahn, per Ausschreibung eine leistungsfähige Security-Lösung für Linux. Beim slowakischen IT-Security-Hersteller ESET wurde sie fündig.

Als internationaler Anbieter von Mobilitäts- und Logistikdienstleistungen agiert der Deutsche Bahn Konzern weltweit in über 130 Ländern. Kern des Unternehmens ist das Eisenbahngeschäft in Deutschland mit über 5,5 Millionen Kunden täglich im Schienenpersonenverkehr und rund 607 Tausend Tonnen beförderter Güter pro Tag. Mehr als 300.000 Mitarbeiter, davon rund 196.000 in Deutschland, setzen sich täglich dafür ein, Mobilität und Logistik für die Kunden sicherzustellen und die dazugehörigen Verkehrsnetze auf der Schiene, Straße, zu Wasser und in der Luft effizient zu steuern und zu betreiben. Die IT-Infrastruktur ist dabei die Basis, mit der die Mitarbeiter der Bahn den täglichen Regelbetrieb absichern.

Heikle Netzübergabe

Die Domäne der Deutschen Bahn umfasst knapp 70.000 Nutzer und stellt IT-Services, Netzwerkzugang und verschiedenste Dienste zur Verfügung. Der Großteil dieser Benutzer hat gleichsam Zugang zum Internet, wodurch das Intranet zum Ziel externer Angriffe werden kann. Um dieses angreifbare Nadelöhr bestmöglich abzusichern und Risiken zu minimieren, muss eine leistungsfähige Gateway-Security-Lösung implementiert sein, die den Netzübergabepunkt der DB zuverlässig schützt.

„Doch durch die guten Erfahrungen mit der ESET Gateway Security werden die Sicherheitslösungen des Unternehmens sicher auch in Zukunft stets berücksichtigt, wenn es um neue Ausschreibungen in diesem Umfeld geht".

DB Systel

Da der Vertrag mit dem bisherigen Gateway-Security-Dienstleister auslief, entschied sich die DB Systel dafür, den neuen Zulieferer über eine Ausschreibung zu bestimmen. Im Rahmen der Ausschreibung offenbarte sich ein überschaubares Marktangebot: Neben ESET waren lediglich zwei weitere Anbieter in der Lage, eine moderne Linux-basierte Gateway Security bereitzustellen.

Neben kaufmännischen Aspekten spielten für DB Systel auch technische Aspekte wie Erkennungsrate, Umfang des Reportings und Performance eine große Rolle bei der Evaluierung der einzelnen Lösungen. Diese Punkte zählen zu den Paradedisziplinen des slowakischen Sicherheitsspezialisten, wie unabhängige Tests immer wieder belegen. Innerhalb von sechs Monaten und damit erheblich schneller als üblich, beschloss die DB Systel, die ESET Gateway Security für Linux einzusetzen. Die Entscheidung basierte dabei auf einem standardisierten Punktekatalog im Rahmen der Ausschreibung – hier konnte ESET am Schluss das beste Ergebnis ausweisen. Den letzten Impuls lieferte aber das gute Preis-Leistungs-Verhältnis der ESET-Lösung.

Stephan Hommel, Niederlassungsleiter Dresden bei der arxes-tolina GmbH, erinnert sich: „Ferdikan Ilyasoglu, Territory Manager bei der ESET Deutschland GmbH, wandte sich mit der Information an uns, dass in naher Zukunft eine neue Gateway-Security-Lösung bei der Deutschen Bahn ausgeschrieben wird. In intensiver Zusammenarbeit mit den Technik- und Finanzabteilungen wurden sämtliche Anforderungen der DB erfüllt." Insbesondere die kaufmännische Abwicklung wurde federführend durch Stephan Hommel in enger Absprache mit Ferdikan Ilyasoglu sowie den weiteren ESET-Mitarbeitern umgesetzt. Stephan Hommel lobte besonders den lokalen deutschen Support von ESET.

ESET Gateway Security: Angenehm unauffällig und leistungsstark

Seit der Implementierung der ESET Gateway Security im September 2015 sind die Verantwortlichen von Leistung der Sicherheitslösung überzeugt. Die ESET Gateway Security arbeitet unauffällig und drängt sich beim Nutzer zu keinem Zeitpunkt in den Vordergrund. Bisher läuft alles wie am Schnürchen: DB Systel konnte keinerlei Unstimmigkeiten im Betrieb feststellen. Den IT-Experten zufolge kommen immer wieder positive Rückmeldungen aus den Fachbereichen, dass die Nutzung des Internet seit der Inbetriebnahme sehr viel bequemer sei als zuvor. Die Bahn-Mitarbeiter verwenden die Lösung mit Freude und loben gegenüber der DB Systel, dass sie den Zugriff auf das Netz weder verlangsamt noch an irgendeiner Stelle spürbar ist.

Starker Rückhalt

Die ESET Gateway Security für Linux läuft im DB Rechenzentrum so ruhig und unauffällig im Hintergrund, dass so mancher Systemadministrator nach der erfolgreichen Inbetriebnahme zeitweise Angst hatte, dass sie gar nicht akkurat laufe. Mehrere Prüfungen zeigen jedoch, dass die Lösung zu jeder Zeit zuverlässig arbeitet.

Genauso positiv verläuft der technische After-Sales-Support. Im Gegensatz zu manchen Mitbewerbern liefert ESET keine Software „von der Stange", sondern passt sie den individuellen Bedürfnissen des Kunden an. So wünschte sich die Deutsche Bahn beispielsweise ein erweitertes Logfile über die Client-IP bei einer Virenerkennung. Die Optimierung wird aktuell getestet und in Kürze implementiert. Weiterhin gab es spezifische Vorstellungen für Konfigurationsmöglichkeiten beim Dateiscan, die in der nächsten Version als neues Feature Einzug halten wird.

Auf die Frage, ob auch bei zukünftigen Security-Projekten ESET eine Option darstelle, antwortet der verantwortliche Projektmanager der DB Systel mit einem klaren „Ja". Sicherheit sei immer ein Thema, ganz besonders für die Deutsche Bahn. Natürlich werde auch künftig stets der gesamte Markt überblickt. „Doch durch die guten Erfahrungen mit der ESET Gateway Security werden die Sicherheitslösungen des Unternehmens sicher auch in Zukunft stets berücksichtigt, wenn es um neue Ausschreibungen in diesem Umfeld geht".

Fall

Im Rahmen der Ausschreibung suchte die Deutsche Bahn eine leistungsfähige Linux-basierte Security-Lösung zur Absicherung der Netzwerksicherheit.

Lösung

Angesichts der speziellen IT-Infrastruktur und Anforderungen fiel die Wahl auf die ESET Gateway Security, die seit 2014 im Einsatz ist.

Benefit

- ➜ *Gutes Preis-Leistungs-Verhältnis*
- ➜ *Hohe Erkennungsrate & Performance*
- ➜ *Detailliertes Reporting*
- ➜ *Bequemes Handling der Lösung*
- ➜ *After-Sales-Support inklusive*


Quelle: Pixabay

Fernwirknetze von Stadtwerken schützen – lückenlos durch Anomalieerkennung

Spätestens seit den Cyberattacken auf ukrainische Energieversorger 2015 und 2016 sind auch in Deutschland Stadtwerke angehalten, ihre Sicherheitsstrategien zu hinterfragen. Das bei einem großen sächsischen Stadtwerk installierte Steuernetz-Überwachungswerkzeug von Rhebo gewährleistet Transparenz und eine lückenlose Meldung jeglicher verdächtiger Aktionen in der Kommunikation von Fernwirknetzen.

Energieversorger und Stadtwerke stehen spätestens seit den Cyberangriffen »WannaCry« und »Industroyer« vor neuen Herausforderungen. Die Steuernetze Kritischer Infrastrukturen sind aus Aspekten der Versorgungs- und Inneren Sicherheit zwar entsprechend der grundlegenden (bekannten) Gefahren konfiguriert und abgesichert. In der Regel beschränken sich die verwendeten Netzwerksicherheitslösungen aber auf Firewalls und eine Trennung der Netzwerke in einzelne Zellen.

Diese Ansätze berücksichtigen weder die wachsende Anzahl unbekannter Gefährdungsvektoren wie z. B. Erpressersoftware, noch die Effekte der zunehmenden Netzwerkkomplexität, die sich aus der Entwicklung durch Industrie 4.0 und dem Industriellen Internet der Dinge (IIoT) ergeben.

Die Herausforderung: Transparenz und umfassende Absicherung in Echtzeit

Im vorliegenden Anwendungsfall des sächsischen Stadtwerkes gab es deshalb drei wesentliche Herausforderungen, die eine zeitgemäße IT-Sicherheitsstrategie beantworten sollte:

1. **Restrisiko durch Cyberangriffe minimieren**
   In dem Stadtwerk waren bereits Firewalls aktiv und gut konfiguriert. Aufgrund der Abhängigkeit von der Gefahrendatenbank der Sicherheitsdienstleister und nicht immer pünktlich eingespielter Updates bestand jedoch stets ein Restrisiko, dass unbekannte Gefahren übersehen werden. Dieses Restrisiko sollte minimiert werden.
2. **Missbrauch der VPN-Zugänge verhindern**
   Die Subunternehmer erhalten für die Fernwartung zahlreiche Autorisierungen. Dadurch existiert das Risiko einer signifikanten Störung des Betriebs beim Missbrauch eines VPN-Zugangs oder bei einer fehlerhaften Eingabe während der Fernwartung. Diese Vorgänge sollen umgehend gemeldet werden, um schnell und effektiv Störungen zu vermeiden.
3. **Vollständige Transparenz des Steuernetzes herstellen**
   Die Firewalls des Stadtwerkes überwachen ausschließlich die Grenzen des Fernwirknetzes. Das Innenleben des Netzwerkes liegt dabei im toten Winkel. Für eine umfassende IT-Sicherheitsstrategie soll jede, auch interne Kommunikation und jede Veränderung dieser lückenlos sichtbar gemacht werden.

Die Lösung: Selbstlernende Anomalieerkennung

Die Administratoren des Stadtwerkes entschieden sich deshalb Anfang 2017 für die Installation der Netzwerksicherheitslösung Rhebo Industrial Protector.

Im Gegensatz zu gängigen Lösungen fokussiert sich Rhebo Industrial Protector nicht ausschließlich auf bekannte Gefahren, sondern detektiert jegliche Veränderung oder Abweichung im Steuernetz. Das erfolgt unabhängig davon, ob die Veränderung bereits als Gefahr definiert oder noch unbekannt ist. Diese sogenannten Anomalien können sowohl Cy-

berangriffe umfassen, als auch verdächtige Operationen durch manuellen Eingriff sowie Netzwerkprobleme.

Dazu wird jedes einzelne Datenpaket, welches im Steuernetz ausgetauscht wird, mittels selbstlernender Deep-Packet-Inspection-Technologie auf Inhaltsebene und in Echtzeit analysiert. Rhebo Industrial Protector kann damit zuverlässig und detailliert die Kernfragen eines Netzbetreibers zur Überwachung der Fernwirk- und Netzleittechnik beantworten:

1. Gibt es neue Kommunikationsteilnehmer?
2. Entstehen neue Kommunikationsverbindungen zwischen Komponenten?
3. Werden neue Protokolltypen verwendet?
4. Verändern sich Autorisierungen oder Befehle zwischen Komponenten?
5. Verändern sich die Kommunikationsflüsse und -häufigkeiten?

Alle Fragen zielen auf Hinweise für Fremdzugriffe und Manipulationsversuche. Zusätzlich werden mit dem 5. Punkt interne Probleme bei der Netzkommunikation wie z. B. durch sporadische Verbindungsausfälle oder Kapazitätsengpässe aufgedeckt. Jede Anomalie wird inklusive aller Rohdaten (im PCAP-Format) für eine spätere forensische Analyse gespeichert.

Der Ansatz dieser automatischen Anomalieerkennung war in dem Stadtwerk sinnvoll, da Fernwirknetze von einer sich wiederholenden und vorhersagbaren Kommunikationsstruktur geprägt sind. Die Leitwartensteuerung des Stadtwerkes folgt klar definierten Befehlsstrukturen und Kommunikationsmustern. Im Gegensatz zur Büro-IT ist somit das automatische Lernen einer Standardkommunikation möglich. Über einen kontinuierlichen Abgleich der aktuell ablaufenden Kommunikation mit diesem Standardmuster können Veränderungen lückenlos erkannt und für die Überprüfung an die Leitwarte gemeldet werden. Der Netzführer hat die Befehlshoheit über alle Meldungen und kann verdächtige Anomalien gezielt freigeben, blockieren und analysieren.

Das Ergebnis: Transparenz und umfassende Absicherung

Im ersten Schritt galt es, die vollständige Transparenz des Fernwirknetzes herzustellen und die gesamte Struktur sichtbar zu machen. Die Leitstelle erlangte über die initiale Analyse erstmals ein vollständiges Verständnis von ihrem Netzwerk, den Geräten sowie deren Befehls- und Kommunikationsstruktur. Auf dieser Basis konnte das Netzwerk grundlegend auf seine Stabilität und Sicherheit überprüft werden und z. B. nicht notwendige oder bislang unbekannte Komponenten und Teilnehmer entfernt werden.

Im laufenden Betrieb werden seitdem alle Abweichungen von den Standardkommunikationsmustern auf einem übersichtlichen Dashboard priorisiert und zur Prüfung angezeigt. So zeigte sich, dass sich die Kommunikation im Steuernetz vorrangig auf einen einzigen Protokolltypen beschränkt. Abweichungen von diesem Protokolltypen werden – mit bekannten Ausnahmen – somit zuverlässig und umgehend gemeldet. Weiterhin werden selbst kleinste funktionelle Änderungen in den Kontrollprotokollen detektiert.

Jegliche Anomalie wird inklusive der Metadaten und Rohdaten für eine spätere forensische Analyse gespeichert. Damit kommt das Stadtwerk auch der Meldepflicht nach dem IT-Sicherheitsgesetz nach.

Das sächsische Stadtwerk hat mit der neuen Netzwerküberwachung zudem ein zuverlässiges Werkzeug, seine Subunternehmer für die Fernwartung besser zu kontrollieren. Störungen durch infizierte Wartungslaptops oder die Verwendung vertraglich nicht autorisierter Netzwerkkomponenten werden in Echtzeit gemeldet. Das erlaubt den Administratoren eine umgehende Kontaktaufnahme mit den Wartungstechnikern und eine Abklärung der Umstände. Da Rhebo Industrial Protector als selbstlernende Software die Kommunikation im Steuernetz dynamisch mitlernt, entsteht mittelfristig auch eine vollständige Transparenz über die Kommunikationsmuster der Wartungsarbeiten.

Rhebo Industrial Protector gewährleistet dem Stadtwerk somit:

- volle Transparenz über alle Teilnehmer und Vorgänge im eigenen Fernwirknetz;
- die detaillierte Echtzeitmeldung jeder Anomalie im Fernwirknetz;
- die Einhaltung der Meldepflicht.

Schlussendlich konnte das Stadtwerk dadurch das Sicherheitsniveau seines Fernwirknetzes signifikant erhöhen und ist auf zukünftige Herausforderungen bestens vorbereitet.

Mit Rhebo Industrial Protector erlangte das Stadtwerk erstmals volle Transparenz über alle Netzwerkteilnehmer und Verbindungen. Die IP-Adressen sind aus Datenschutzgründen unkenntlich gemacht. (Quelle: Rhebo)

Klaus Mochalski, CEO, Rhebo GmbH (https://rhebo.com)

Verschlüsselungs-Trojaner: Schnelle Hilfe durch Emergency-Team

Theoretisch ist wohl jedem klar, dass auf die Forderungen von Erpressern nicht eingegangen werden sollte. Im praktischen Leben ist das nicht ganz so einfach: Mit Verschlüsselungs-Trojanern gelingt es Cyberkriminellen immer wieder, Unternehmen schwer zu schädigen. Dabei sind keineswegs nur große, namhafte Firmen betroffen, wie ein aktuelles Beispiel aus Norddeutschland zeigt. Dank einer IT-Sicherheits-Strategie sowie der Unterstützung durch den IT-Dienstleister mod IT Services gelang es, das befallene System schnell zu isolieren, größeren Schaden zu verhindern und das Problem ganzheitlich zu betrachten.

„Eine gute Vorbereitung, eine ganzheitliche Analyse verbunden mit einer schnellen Reaktion, sind die maßgeblichen Dinge, die bei der Abwehr eines Trojaners helfen", sagt Andreas Scharf, Security-Spezialist bei dem IT-Dienstleister mod IT Services. „Der Schaden, bestehend aus möglicherweise gezahltem Lösegeld, Datenverlust, Systemausfall und nicht zuletzt Image-Verlust kann schnell existenzgefährdend werden."

In den letzten Jahren machten Verschlüsselungs-Trojaner immer wieder Schlagzeilen. Waren bisher vor allem Privatleute betroffen, geraten nun vermehrt Unternehmen ins Visier der Hacker.

Schadensbegrenzung und umfassender Check

„Ein mittelständisches Produktionsunternehmen aus Norddeutschland wurde jüngst Opfer einer Verschlüsselungs-Trojaner-Attacke", erzählt Andreas Scharf. Mit einer Bewerbungs-E-Mail, die der User geöffnet hatte, war die Schadsoftware in die Unternehmens-Infrastruktur gelangt. Das Unternehmen ist dank der proaktiven Beratung durch mod IT Services für derartige Fälle sensibilisiert und arbeitet mit einem umfassenden IT-Security-Konzept.

Schon die Erst-Analyse des Supports ließ einen Trojaner-Befall vermuten. „An dieser Stelle mussten wir sofort und nachhaltig handeln, um den Schaden so gering wie möglich zu halten", erläutert Andreas Scharf. Das Emergency-Team von mod IT Services übernahm alle technischen und organisatorischen Maßnahmen: Es isolierte das befallene System, um Übergriffe auf die Server zu verhindern, sicherte Beweise und startete sofort mit der Fehleranalyse. „Wir mussten zunächst den sogenannten ‚Patient Null' ermitteln – das System, zu dem die nun verschlüsselten Daten gehören. Nach einem umfassenden Check der restlichen Infrastruktur konnten alle anderen User schnell wieder arbeiten." Größerer finanzieller Schaden oder Datenverlust konnte so verhindert werden.

Sich nicht überraschen lassen

„Einen Verschlüsselungs-Trojaner einzuschleusen ist eine Straftat", sagt Andreas Scharf. „Betroffene sollten den Vorfall deshalb dem BSI melden." Im konkreten Fall des norddeutschen Mittelständlers übernahm mod IT Services die Zusammenarbeit mit der Polizei und erntete dafür die Anerkennung der Beamten: „Wir haben der Polizei die notwendigen Informationen zusammengestellt und so aufbereitet, dass die Fahnder schnell die Arbeit aufnehmen konnten." Das befallene System wurde schließlich neu aufgesetzt, das aktuelle Backup eingespielt.

Auf die Frage, was er Unternehmen im Kampf gegen Verschlüsselungs-Trojaner empfehlen würde, antwortet Andreas Scharf: „Man kann solche Angriffe nie hundertprozentig verhindern oder vorhersehen, aber man kann vorbereitet sein. Entsprechend sensibilisierte Mitarbeiter und ein ganzheitliches Security-Konzept sind die Basis und nicht zuletzt die professionelle Unterstützung durch das mod IT Services Emergency-Team, wenn Schadware festgestellt wird."

Andreas Scharf,
Security-Spezialist,
mod IT Services

Elektronische Datenträger physisch vernichten (lassen)

Bei der Entsorgung von digitalen Datenträgern ist Vorsicht geboten, denn unzählige vertrauliche Daten sind auf unseren Computern, USB-Sticks, CDs und DVDs etc. gespeichert und stellen vor allem für Unternehmen ein Sicherheitsrisiko dar. Doch was passiert mit diesen Speichermedien am Ende ihres Lebens? Das Bundesamt für Datensicherheit spricht hier eine eindeutige Empfehlung aus, bei Festplatten gilt die Devise „ausbauen und physisch zerstören".

Durch das Schreddern der Festplatten wird ausgeschlossen, dass der Datenträger jemals wieder korrekt zusammengebaut werden kann. Mittels Schneidwellen aus schwerem Stahl werden die Festplatten zerquetscht und zerkleinert – ein Vorgang ähnlich dem Schreddern von Papier. Wer große Mengen von Festplatten zu löschen hat oder die Festplattenvernichtung als Dienstleistung anbieten möchte, kommt nicht darum herum, einen Festplattenvernichter zu kaufen.

Das Potenzial bei der Vernichtung von digitalen Datenträgern hat Theodor Andres, Inhaber und Geschäftsführer der Andres Büro- und Kopiersysteme GmbH in Bergheim, bereits 2013 erkannt und bietet seinen Kunden seitdem nun die Möglichkeit, neben Festplatten auch andere digitale Datenträger, wie beispielsweise CDs, USB-Sticks, Magnetbänder etc. professionell zu vernichten. Dafür hat Theodor Andres damals in den Festplattenvernichter „HSM Powerline HDS 230" des Herstellers HSM investiert, da laut seiner Aussage HSM in diesem Bereich einen sehr guten Ruf als Hersteller besitzt und er bereits seit vielen Jahren mit HSM eine partnerschaftliche Beziehung pflegt, denn die Firma Andres Büro- und Kopiersysteme bietet seit einigen Jahren einen mobilen Aktenvernichter-Service an, bei dem bereits Großaktenvernichter der Firma HSM zum Einsatz kommen. „Wir haben die gute Qualität ,"Made in Germany", den Service und das gute Preis-Leistungsverhältnis der Firma HSM kennen und schätzen gelernt und uns deshalb für diesen Festplattenvernichter entschieden", sagt Andres. Um immer auf dem neuesten Stand der Normen und Gesetze zu sein, besuchen seine Mitarbeiter regelmäßig bei HSM Schulungen zu den Themen Datenschutz und Datensicherheit.

Theodor Andres, Inhaber der Andres Büro- und Kopiersysteme GmbH legt beim Vernichten der Festplatten selbst Hand an

Inzwischen nutzen einige Stammkunden die Dienstleistung, dazu gehören unter anderem Verbände, Krankenhäuser, EDV-Unternehmen usw. Eingrenzen lassen sich die Zielgruppen kaum, da nahezu in jeder Branche personenbezogene Daten auf Festplatten etc. gespeichert werden, vor allem in Banken, Versicherungen, im medizinischen und rechtwissenschaftlichen Bereich, aber auch in Verwaltungen und Behörden ist besondere Aufmerksamkeit geboten. „Heutzutage werden alle geschäftskritischen Daten, Informationen und Berichte in digitaler Form auf PCs, sprich Festplatten, abgelegt. Dabei machen sich die Firmen durchaus Gedanken über Themen wie Firewalls, WEB-Filter oder Anti-Virus Software", sagt Andres. „Die datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger wird allerdings sträflich vernachlässigt." Dabei sind die Unternehmen durch das Bundesdatenschutzgesetz zum verantwortungsvollen und korrekten Umgang mit personenbezogenen Daten verpflichtet. D.h. Datenträger müssen so vernichtet werden, dass die Reproduktion der Daten, je nach Inhalt, unmöglich oder weitestgehend erschwert wird. Die DIN-Norm 66399 berücksichtigt die Vielfalt der digitalen Datenträger und definiert die Sicherheit für alle zeitgemäßen Medien. Mit dem Festplattenvernichter HSM Powerline HDS 230 erreicht Theodor Andres die Schutzklasse 3 und die Sicherheitsstufe H-5 und erfüllt damit voll und ganz die Norm, da die Datenträger in Partikel mit einer Größe von maximal 320 Quadratmillimetern zerteilt werden. Die Edelmetalle aus den Festplatten lassen sich zudem umweltgerecht recyceln.

HSM GmbH + Co. KG
Austraße 1-9
88699 Frickingen / Germany
Tel. +49 7554 2100-0 • Fax: +49 7554 2100-160
Internet: www.hsm.eu • E-Mail: info@hsm.eu

SN 200 Firewall von Stormshield

Stormshield Network Security sichert Bildungsnetzwerk bei Digitale Helden gGmbH
Practise what you preach: höchste Datensicherheit für Digitale Helden

Cybermobbing ist ein Problem an vielen Schulen. Diesem Thema nehmen sich seit 2014 die Digitalen Helden an. Das gemeinnützige Start-up aus Frankfurt am Main vermittelt Medienkompetenz sowie digitale Bildung an Schulen und in Familien. Seit der Gründung des erfolgreichen Start-ups wächst das Team ständig weiter. Mit dem Unternehmen wuchs auch das Bedürfnis, die eigene Datensicherheit und den Workflow zu professionalisieren. Heute schützen die Digitalen Helden ihr Netzwerk mit Stormshield Network Security.

Das Team der Digitalen Helden besteht derzeit aus sieben Festangestellten. Hinzu kommen zehn Freiberufler, mit denen das junge Unternehmen bei Bedarf zusammenarbeitet. Für die Workshops und Seminare der Digitalen Helden muss das Unternehmen Lehrinhalte online zur Verfügung stellen und den Zugriff von außen auf die Infrastruktur gewährleisten. Für Veranstaltungen in den Räumlichkeiten der Digitalen Helden ist die Arbeit im Intranet unerlässlich.

„Heldenhafter" Schutz gesucht

Digitale Helden setzen hierfür auf eine zweigeteilte Infrastruktur: Im Intranet wird gearbeitet und auf das Internet zugegriffen. Über einen VPN-Tunnel können die Angestellten dies auch von unterwegs nutzen. Hier werden unter anderem Kontaktdaten von Partnern, Schulen, etc. verwaltet. Der Zugriff von außen muss also streng reguliert sein.
Der zweite Teil der Infrastruktur ist eine „demilitarisierte Zone" (DMZ), ein vom Intranet getrenntes Netzwerk. Hier sind zum Beispiel File Sharing-Dienste angesiedelt. Durch die Trennung der Netzwerke bleibt das Intranet sicher, wenn beispielsweise die DMZ angegriffen wird. Mit dem Wachstum des Start-ups kam bei den Digitalen Helden auch der Wunsch auf, die eigene IT-Sicherheit zu erhöhen. „Datenschutz, Privatsphäre, Datenhoheit und Datensicherheit sind uns ein hohes Anliegen, das wir u.a. auch an junge Menschen vermitteln", erklärt Jörg Schüler, einer der zwei Geschäftsführer bei Digitale Helden. „Mit dem Wachstum unseres Unternehmens stieg bei uns das Bedürfnis, unsere Datensicherheit und den Workflow zu professionalisieren und zu zentralisieren – Practise what you preach."

Höchste Leistung auch für KMU

Das Team der Digitalen Helden war also auf der Suche nach einer Netzwerksicherheitslösung, die zu der Infrastruktur der gemeinnützigen GmbH passt. Schließlich fiel die Wahl auf die Firewall „SN 200" des europäischen Herstellers Stormshield, dessen Technologien in Europa auf höchster Ebene zertifiziert wurden und unter anderem für den Einsatz in der EU und der NATO zugelassen sind. Mit einem Datendurchsatz von 600 Mbps reicht die Leistung der „SN 200" für die Digitale Helden aus. Die Lösung ist modular einsetzbar und somit für künftige Änderungen der Infrastruktur gewappnet. Durch VPN SSL eignet sie sich besonders für „Bring your own device" (BYOD)-Strategien. Die Mitarbeiter können also auch von unterwegs mit ihren privaten Geräten, auf die Unternehmensdaten zugreifen. Die Konfiguration erfolgte schnell und unkompliziert über die Administratorenschnittstelle. Sollte die SN 200 ausfallen, hilft der Stormshield Service weiter.

Fazit

Die Infrastruktur der Digitalen Helden wird professionell geschützt. Eine moderne BYOD-Strategie ist mit höchsten Sicherheitsstandards möglich. Das Unternehmen vermittelt Jugendlichen Medienkompetenz und ein Bewusstsein für Datensicherheit im Netz. Da muss die Sicherheit der eigenen Systeme der Außendarstellung entsprechen. Und wenn einmal Jugendliche während eines Lehrganges fragen, wie Digitale Helden die eigenen Netze sichert, genügt die eigene Lösung nicht nur allerhöchsten Ansprüchen, sondern ist durch ihre Hardware gewissermaßen eine Lösung zum Anfassen.

Weitere Informationen zu Digitale Helden auf: www.digitale-helden.de.
Weitere Informationen zu Stormshield auf: www.stormshield.eu.

controlware
communicationssysteme

Web Application Firewalling und Load Balancing

Paragon Data setzt beim Schutz von Web-Anwendungen auf Controlware

Controlware, renommierter deutscher Systemintegrator und Managed Service Provider, unterstützte den IT-Dienstleister Paragon Data bei der Integration einer leistungsfähigen Web Application Firewall (WAF) für einen seiner IaaS-Kunden. Die innovative neue Security-Plattform vereint zuverlässigen Schutz auf Anwendungsebene mit leistungsfähigem Load Balancing und gewährleistet so den effizienten und sicheren Betrieb kritischer Web-Anwendungen.

Im März 2016 entschied sich ein wichtiger Hosting-Kunde von Paragon Data, seine SOAP-basierte Kundenanbindung auf eine webbasierte Architektur zu verlagern. Die Migration war mit Blick auf die Effizienz und Zukunftssicherheit der IT ein zukunftsweisender Schritt, doch unter Sicherheitsgesichtspunkten zunächst eine enorme Herausforderung: Die kritischen neuen Systeme sollten vor webbasierten internen und externen Attacken geschützt werden – und das konnten die vorhandenen Firewalls alleine nicht leisten.

„Die Bedrohungslandschaft verlagert sich zunehmend auf die Applikationsebene. Schon heute erfolgen 70 bis 80 Prozent aller Cyberangriffe auf Layer 7 und sind für portbasierte Firewalls nicht zu stoppen", erläutert Alexander van de Poll, Bereichsleiter Systemtechnik und Rechenzentren bei Paragon Data. „Klassische Firewalls verlieren damit zunehmend an Bedeutung. Wir waren uns mit unserem Kunden daher von der ersten Minute an einig, dass eine leistungsfähige WAF zum Schutz seiner kritischen, webbasierten Business-Anwendungen unabdingbar ist. Gemeinsam mit unserem langjährigen Partner Controlware machten wir uns auf die Suche nach einer zukunftssicheren und skalierbaren Lösung."

Optimaler Schutz für Anwendungen

Ziel des Projekts war es, mithilfe einer dedizierten Web Application Firewall eine zusätzliche, auf konsequentem Whitelisting basierende Schutzschicht für Web-Anwendungen zu integrieren. Dabei sollte die Lösung Angriffsmuster automatisch erkennen und stoppen, um den Anwendungsentwicklern bei einem Angriff mehr Zeit für die Aktualisierung der Systeme zu sichern und die Zeit bis zum Update zu überbrücken. Ausgehend von diesem Anforderungskatalog fokussierte sich das Projektteam auf das Lösungsportfolio von F5 Networks:

- Paragon Data schätzt die F5 BIG-IP-Plattform als zuverlässige leistungsfähige Lösung, da man seit längerem mehrere BIGIP 3600 sowie BIG-IP 3900 im Einsatz hat.
- Die Lösung ist modular aufgebaut. Sie kann unter anderem sowohl mit einer WAF, dem Application Security Manager (ASM), als auch einem Load Balancer, dem Local Traffic Manager (LTM), ausgerüstet werden. Paragon Data bildet so alle benötigten Funktionalitäten auf einer Appliance ab.

„Die Plattform hat sich als bedienfreundlich, zuverlässig und flexibel erwiesen. Wir erreichen ein hohes Maß an Sicherheit."
Jacek Dubiel, Projektleiter und Abteilungsleiter Netzwerk und Sicherheit bei Paragon Data

- Im Gegensatz zu den Produkten anderer Hersteller stellt die Lösung eine ganzheitliche Architektur zur DoS- und DDoS-Abwehr bereit. Angesichts der rasanten Zunahme großangelegter Attacken war dies ein zentrales Auswahlkriterium.
- Die Lösung bietet erhebliche wirtschaftliche Vorteile: Die vorhandene Plattform konnte auf Anraten von Controlware im Rahmen eines Hardware-Refreshs kostengünstig durch ein neues Modell ersetzt werden.

„Unsere Netzwerkexperten haben den aktuellen Bandbreitenbedarf bei Paragon Data und beim Endkunden analysiert und daraus eine tragfähige Prognose für die künftigen Durchsatzanforderungen erstellt", erklärt Wolfgang Essel, Security Consultant bei Controlware. „Paragon hat sich dann in Absprache mit dem Kunden für die von uns empfohlene kompakte BIG-IP 2000s mit einem Layer-7-Durchsatz von 5 Gbps und rund 75.000 Layer-4-Verbindungen pro Sekunde entschieden – eine äußerst zukunftssichere und performante Plattform."

Optimale Anwendungsperformance

Die neue BIG-IP-Hardware wurde im Data Center von Paragon Data in Betrieb genommen. Darauf installiert ist ein Local Traffic Manager (LTM), der die durchgängige Verfügbarkeit der kritischen Anwendungen sicherstellt. Der leistungsstarke Load Balancer verteilt hierfür eintreffende Web-Anfragen auf die vorhandenen Ressourcen und garantiert während der Lastspitzen stabile Performance-Werte. Auch bei der Abwehr von DDoS-Attacken kommt dem LTM eine Schlüsselrolle zu: Wenn er erkennt, dass ein Angreifer die Systeme unter einer Flut von Anfragen in die Knie zwingen will, leitet er legitime Verbindungen auf nicht überbelastete Ressourcen um.

WAF-Policy mit Whitelisting

Ebenfalls auf der BIG-IP-Plattform implementiert ist das Modul Application Security Manager (ASM). Die Web Application Firewall nimmt den Web-Traffic entgegen, entschlüsselt SSL-Verbindungen und prüft, ob die Inhalte der hinterlegten Policy entsprechen oder eine Gefahr darstellen. Dabei folgt die WAF-Richtlinie einem konsequenten Whitelisting-Ansatz: „Wir haben mit dem Entwickler der Web-App definiert, welche URLs und Parameter in welchem Format legitim sind – und die WAF so konfiguriert, dass ausschließlich diese Anfragen zugelassen werden", erklärt Jonas Teckentrup, Administrator Netzwerk und Sicherheit bei Paragon Data. „So lassen sich gängige Angriffe auf Anwendungsebene, vom Cross-Site-Scripting über SQL-Injections bis hin zu Click Jacking oder CSRF-Attacken, bestmöglich unterbinden."

Zusätzlich stellt der ASM eine Reihe weiterer Security-Funktionalitäten bereit:

- Blockieren bekannter Angriffssignaturen: Die Signaturdatenbank wird regelmäßig aktualisiert. Um False Positives zu vermeiden, werden neue Regeln erst nach Freigabe durch den Administrator in das aktive Regelwerk übernommen.
- Intelligente DoS-Protection: Die WAF erkennt und blockiert schädliche Zugriffsversuche über DoS-Tools, E-Mail-Kollektoren, Exploit-Tools, Netzwerk-Scanner, Spam-Bots, Web-Spider, Vulnerability-

Paragon Data GmbH

Paragon Data mit Sitz in Friedrichsdorf bei Frankfurt am Main ist ein innovativer IT-Dienstleister im Konzernverbund der DBH Buch Handels GmbH & Co. KG. Paragon Data betreibt das Rechenzentrum des Mutterkonzerns und unterstützt mehr als 100 Filialen – jede davon mit bis zu 80.000 vorrätigen und über 10 Millionen bestellbaren Artikeln – mit einer leistungsstarken, sicheren und stabilen IT-Infrastruktur. Darüber hinaus erbringt Paragon Data für konzerninterne und externe Kunden zentrale Dienstleistungen wie Beratung, Anwendungsentwicklung, Servicedesk, Rechenzentrumsbetrieb und viele mehr. Über 60 Mitarbeiter an den Hauptstandorten Friedrichsdorf und München bilden ein eingespieltes und hoch motiviertes Team von Fachleuten. Flache Hierarchien, eine offene Kommunikation und Flexibilität sind Teil der Unternehmenskultur. Paragon Data unterstützt seine Kunden bei der Implementierung und dem Betrieb ihrer IT-Landschaft. Langjährige Erfahrung mit Schwerpunkten im technischen Filial-Management sowie Oracle-Consulting und Hosting bilden die Säulen des Erfolgs – strenge Qualitätssicherung die Basis der Arbeit.

„Angesichts der positiven Erfahrungen mit der BIG-IP-Plattform planen wir, die Lösung 2017 auch als Managed Service anzubieten."
Alexander van de Poll, Bereichsleiter Systemtechnik und Rechenzentren bei Paragon Data

„Wir haben die WAF so konfiguriert, dass ausschließlich legitime Anfragen zugelassen werden. So lassen sich gängige Angriffe auf Anwendungsebene bestmöglich unterbinden."
Jonas Teckentrup, Administrator Netzwerk und Sicherheit bei Paragon Data

Scanner und viele mehr. Dabei unterscheidet sie zwischen zulässigen und unzulässigen Zugriffen von Botnetzen: Während bekanntermaßen gefährliche Bots zuverlässig gestoppt werden, sind Bots von Wissensnetzwerken (z. B. Wikipedia), Suchmaschinen (z. B. Google), Monitoring-Systemen (z. B. Nagios) und Social Media (z. B. Facebook) auf einer Whitelist hinterlegt. So lassen sich sowohl volumenbasierte als auch stressbasierte Angriffe unterbinden.

- Parameter- und Zeichensatzprüfung: Um Cross-Site-Scripting (XSS) zu verhindern, überwacht der ASM die Eingaben in Formfeldern, Headern und Metadaten, die Häufigkeit der Eingabe kritischer Parameter (Benutzername und Passwort) und den Zeichensatz des Anwenders. Weisen die Anzeichen auf einen DoS-Angriff hin, leitet die WAF automatisch eine mehrstufige Mitigation ein: Bei einem drastischen Anstieg der Anfragen um rund 500 % werden im ersten Schritt die Anfragen der verdächtigen Benutzer und im zweiten alle internationalen Anfragen gedrosselt. Im dritten Schritt müssen Benutzer vor dem Web-Zugriff ein CAPTCHA eingeben. In der vierten und letzten Stufe lehnt das System Verbindungsanfragen für bestimmte Teile der Website generell ab.

Paragon Data betreibt das Rechenzentrum des Mutterkonzerns, der DBH Buch Handels GmbH & Co. KG, und unterstützt mehr als 100 Filialen – jede davon mit bis zu 80.000 vorrätigen und über 10 Millionen bestellbaren Artikeln – mit einer leistungsstarken, sicheren und stabilen IT-Infrastruktur.

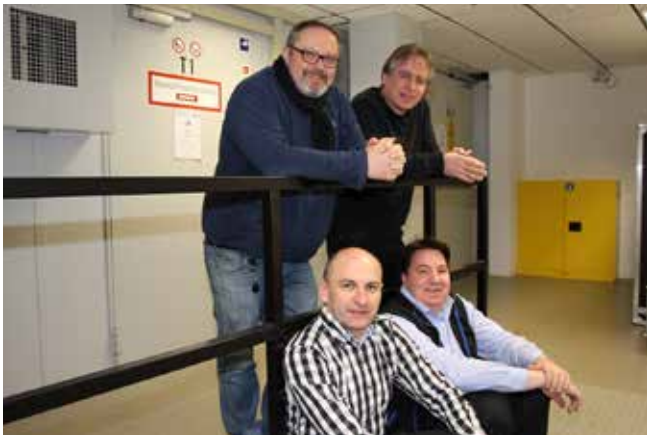
WAF-Workshop für die Mitarbeiter

Nach der Inbetriebnahme und Integration der BIG-IP-Plattform im Juli 2016 stand zunächst ein kontinuierliches Feintuning der Plattform im Fokus, bei dem das Team Performance und Filter optimierte. Parallel dazu schulte Controlware die Mitarbeiter von Paragon Data bei einem Workshop im Management der Web Application Firewall, in der Policy-Pflege und in der Optimierung der Konfiguration. „Die Plattform hat sich vom ersten Tag an als bedienfreundlich, zuverlässig und flexibel erwiesen. Und durch die Whitelisting-Policy erreichen wir ein hohes Maß an Sicherheit, ohne mit False Positives zu kämpfen oder hochkomplexe Regelwerke zu pflegen", so Jacek Dubiel, Projektleiter und Abteilungsleiter Netzwerk und Sicherheit bei Paragon Data. „Durch die Kombination aus WAF und Load Balancer haben wir zudem einen zuverlässigen Schutz vor DDoS-Attacken integriert. Unser Kunde hat so die Gewissheit, dass seine Anwendungen vor internen und externen Angriffen gleichermaßen gut geschützt sind."

WAF künftig auch als Managed Service

Seit dem erfolgreichen Projektabschluss hat Paragon Data das Security-Portfolio kontinuierlich erweitert und den Fokus von der reinen Perimeter-Security auf die Application-Security ausgeweitet. Die Installation wurde sukzessive um neue Komponenten ausgebaut – etwa um ein VPN zur Anbindung großer Kunden. In Zukunft soll auch ein Privileged Account Management für die sichere Anbindung der Administratoren integriert werden. „Angesichts der positiven Erfahrungen, die wir mit der BIG-IP-Plattform gemacht haben, planen wir, die Lösung 2017 auch als Managed Service anzubieten", erläutert Alexander van de Poll. „Viele unserer Kunden würden diesen zusätzlichen Schutz – Web Application Firewall gepaart mit einem performanten Load Balancing – sehr gerne in Anspruch nehmen. Das mit Controlware realisierte Projekt ist eine hervorragende Basis, um unsere Aktivitäten weiter zu intensivieren.

Das Projektteam: Alexander van de Poll (hinten links), Jonas Teckentrup (vorne rechts), und Jacek Dubiel (vorne links) von Paragon Data mit Wolfgang Essel von Controlware.



Klinikum Fulda trotzt Locky & Co. mit Advanced Threat Protection Framework von Fortinet

Zum Schutz vor immer ausgefeilteren Sicherheitsbedrohungen hat das Klinikum Fulda seine vorhandene Security-Infrastruktur erweitert. Neben Next Generation Firewall und Secure E-Mail Gateway gehört dazu heute auch eine Sandbox-Lösung von Fortinet. Die Infrastruktur, die gemeinsam mit dem IT-Partner VINTIN implementiert wurde, schützt damit auch vor Zero-Day-Attacken und Ransomware wie Locky & Co.

Das Klinikum Fulda ist das moderne und leistungsstarke Krankenhaus der Maximalversorgung in Osthessen. Mit mehr als 1.000 Betten in der stationären Versorgung und einem breiten Angebot an spezialisierten Sprechstunden sowie Ambulanzen stellt es die qualitativ hochwertige medizinische Versorgung für die mehr als 500.000 Bürgerinnen und Bürger der Region sicher.

Jedes Jahr werden in den Einrichtungen des Klinikums über 100.000 Patientinnen und Patienten behandelt – 40.000 davon stationär – und von mehr als 2.700 hochqualifizierten Mitarbeiterinnen und Mitarbeitern betreut. Die 25 Kliniken und Institute bieten in fachabteilungsübergreifenden Zentren medizinische Leistungen mit modernsten Behandlungsmethoden, die auch den Vergleich mit Universitätsklinika standhalten.

Als Campus Fulda der Universitätsmedizin Marburg ist das Klinikum Fulda in die neuesten Entwicklungen der medizinischen Forschung eingebunden.

Hochleistungsmedizin setzt sichere IT-Systeme voraus

Ohne moderne IT-Systeme ist das vielfältige Behandlungsangebot im Klinikum Fulda heute nicht mehr vorstellbar. Daher müssen auch die Sicherheitslösungen zum Schutz der IT-Infrastruktur höchste Anforderungen erfüllen. Die IT-Organisation des Klinikums sieht dabei aktuell vor allem drei Herausforderungen: „Zum einen nehmen wir neuartige Bedrohungen wie Ransomware sehr ernst und benötigen entsprechende Schutzmaßnahmen", sagt Diplom-Informatiker Christoph Schneider, der in der IT-Abteilung des Klinikums für Netzwerksicherheit und Datenschutz verantwortlich ist.

„Eine weitere Herausforderung ist die sichere Integration von Systemen im Bereich der Medizintechnik. Hier geht es darum, die medizintechnischen Geräte vom übrigen Netzwerk abzuschotten und gleichzeitig den im Gesundheitswesen geforderten Datenaustausch zu ermöglichen. Und schließlich müssen wir uns mit einem veränderten Benutzerverhalten auseinandersetzen. Anwender nutzen die Möglichkeiten der Informationstechnologie heute ganz selbstverständlich im Privatleben, ohne sich Gedanken über Sicherheit und Datenschutz zu machen. Dies müssen wir bei der Planung unserer Security-Strategie ebenfalls berücksichtigen."

Die IT-Organisation des Klinikums Fulda investiert daher nicht nur in leistungsfähige Sicherheitstechnologien, sondern setzt auch konsequent auf Awareness-Maßnahmen, um die Anwender für mögliche Risiken zu sensibilisieren: „Wir haben unseren Mitarbeitern beispielsweise erklärt, warum Web-Mail-Dienste und Filesharing-Services wie Dropbox im internen Netzwerk gesperrt sind", sagt Christoph Schneider. „Uns ist wichtig, dass sie verstehen, welche Gefahren von diesen Diensten für die Sicherheit unseres Netzwerks ausgehen können."

FortiGate-Cluster vereint unterschiedliche Security-Technologien

Gleichzeitig hat die IT-Abteilung mit Unterstützung des IT-Dienstleisters VINTIN eine ganzheitliche Sicherheitsinfrastruktur aufgebaut, die sowohl bekannte als auch neuartige Gefahren zuverlässig abwehrt. Ein zentraler Baustein der Security-Architektur ist das hochverfügbare FortiGate 1200D-Cluster in den beiden Rechenzentren des Klinikums.

Die leistungsfähigen Next Generation Firewalls von Fortinet schützen die IT-Umgebung in Echtzeit vor

Netzwerk- und Content-basierenden Bedrohungen. Neben marktführender Firewall-Technologie vereinen die Appliances auf einer Plattform

unterschiedliche Sicherheitskomponenten wie zum Beispiel Anti-Malware, VPN, Intrusion Prevention und Web-Filtering. Zudem zeichnet sich die FortiGate-Plattform durch herausragende Performance und Skalierbarkeit aus. Speziell entwickelte FortiASIC-Prozessoren beschleunigen Funktionen wie das Content Scanning und sorgen dafür, dass hohe Netzwerksicherheit nicht zu Lasten des Datendurchsatzes geht.

Anfang 2016 hat VINTIN die aktuellen FortiGate-Systeme im Klinikum Fulda implementiert. Die neuen Appliances verfügen bereits über 10 GbE-Interfaces und bieten damit auch die benötigte Bandbreite für die interne Netzwerkabsicherung.

„Wir setzen die FortiGate-Systeme auch als interne Firewalls ein und haben so Netzwerksegmente für die Medizintechnik und die Haus- und Gebäudetechnik vom übrigen IT-Netzwerk getrennt", erklärt Christoph Schneider. „Mit dieser LAN-Segmentierung kommen wir heute bereits den Anforderungen des neuen IT-Sicherheitsgesetzes nach und bieten zusätzlichen Schutz für kritische medizintechnische Geräte. Die FortiGate-Systeme ermöglichen eine sichere Kommunikation zwischen den verschiedenen Netzwerksegmenten – ohne Einbußen bei der Performance."

Ein weiterer Baustein in der Sicherheitsarchitektur des Klinikums ist das Secure E-Mail-Gateway FortiMail. auch beim Schutz vor Spam-Mails und Malware, die via E-Mail verbreitet wird, entschieden sich die IT-Verantwortlichen für eine Fortinet-Lösung. Neben der einheitlichen Benutzeroberfläche und dem umfassenden Funktionsumfang war dabei das nahtlose Zusammenspiel mit der FortiGate-Plattform ausschlaggebend.

Wenn die FortiMail-Lösung einen Absender von Spam-Mails identifiziert, wird diese Information automatisch an das FortiGate-System weitergegeben und die Adresse ab sofort geblockt. Die FortiMail-Lösung filtert aber nicht nur Spam-Mails aus dem eintreffenden E-Mail-Verkehr, sondern überprüft auch die ausgehenden E-Mails. Outbound Inspection-Technologien von Fortinet verhindern, dass potentielle Schadsoftware über die E-Mail-Server des Klinikums versendet wird – und die Organisation so auf den Blacklists anderer Gateways landet.

Sandbox-Lösung zum Schutz vor Ransomware

„FortiMail fängt Spam und E-Mails mit bekannter Malware sehr zuverlässig ab, bietet allerdings keinen vollständigen Schutz vor hochentwickelten E-Mail-Bedrohungen", berichtet Christoph Schneider. „Für die Abwehr von Ransomware und anderen neuartigen Attacken wurde uns der Einsatz einer FortiSandbox empfohlen."

Die Sandbox-Lösung von Fortinet analysiert verdächtige Dateien wie Office-Dokumente, PDFs oder ZIP-Archive in einer geschützten Umgebung und gibt nur unbedenkliche Dateien für den Anwender frei. Schädliche Elemente werden automatisch blockiert und entsprechende Warnungen an das Sicherheits-Ökosystem von Fortinet übermittelt. FortiSandbox schützt damit sehr effektiv vor Zero-Day-Attacken und anderen Angriffen, die von traditionellen Sicherheitslösungen nicht entdeckt werden.

„Viele Attacken auf unser Netzwerk sind mittlerweile ausgesprochen raffiniert getarnt" sagt Christoph Schneider. „Vor kurzem erreichte uns beispielsweise per E-Mail ein Bewerbungsschreiben mit einem angehängten Lebenslauf. Die Analyse in der Sandbox-Umgebung zeigte, dass es sich bei dem Attachment nicht um ein PDF-File, sondern um eine mit Malware verseuchte Datei handelte.

Die FortiSandbox blockierte den Anhang und verhinderte so, dass ein Anwender das Attachment versehentlich öffnet und so unser Netzwerk mit Schadcode infiziert." Die FortiSandbox arbeitet nicht nur mit FortiMail zusammen, sondern lässt sich auch mit der FortiGate-Plattform verbinden. Auf diese Weise können beispielsweise auch sämtliche Web-Downloads proaktiv auf verdächtige Dateien überprüft werden. Wenn die Sandbox-Lösung dabei Malware identifiziert, werden die Web-Filter des FortiGate-Clusters automatisch angepasst.

Sicherheitsarchitektur hält mit wachsenden Anforderungen Schritt

Um die Leistung der FortiSandbox bei Bedarf ?exibel skalieren zu können, wurde die Lösung als virtuelle Appliance im Rechenzentrum des Klinikums implementiert. „Die Anfangsinvestition war dadurch für uns niedriger als bei einer physischen Appliance – und bei steigenden Anforderungen fügen wir einfach zusätzliche Serverressourcen hinzu", sagt Christoph Schneider. „Zusätzlich profitieren wir von erhöhter Ausfallsicherheit, da wir die virtuelle Appliance sehr schnell im laufenden Betrieb auf andere Hardware verschieben können."

Der IT-Experte sieht das Klinikum Fulda mit den implementierten Technologien sehr gut für die aktuellen Sicherheitsanforderungen gewappnet: „Die einzelnen Fortinet-Komponenten spielen sehr gut zusammen und bilden zusammen eine Sicherheitsarchitektur, die mit den neuen, hochentwickelten Bedrohungen Schritt hält. Zudem haben wir mit FortiAnalyzer eine zentrale Lösung für Logging und Reporting eingerichtet. Damit haben wir alle Sicherheitsthemen immer im Blick und können jederzeit individuelle Analysen und Berichte erstellen, die uns bei der Weiterentwicklung unserer Security-Strategie helfen."

www.fortinet.de

Eckdaten

Kunde: Klinikum Fulda
Branche: Gesundheitswesen
Standort: Fulda
Nutzungsszenario: Absicherung des Netzwerks eines modernen Krankenhauses

Vorteile

- **Aufbau einer ganzheitlichen Sicherheitsinfrastruktur**
- **Zuverlässige Abwehr bekannter und neuer Gefahren**
- **Sichere Integration von Systemen im Bereich der Medizintechnik**
- **Hervorragende Performance und Skalierbarkeit**
- **Sichere Kommunikation zwischen den verschiedenen Netzwerksegmenten**

Verband der Ersatzkassen setzt auf Verschlüsselung von Rohde & Schwarz Cybersecurity

Sozialversicherungsdaten – beispielsweise Name, Geburtsdatum oder Familienstand – sind vom Gesetz besonders geschützt. Um die Datenübertragung zu seinem zweiten Rechenzentrumsstandort entsprechend weiter abzusichern, suchte der Verband der Ersatzkassen e.V. (vdek) in Berlin über eine bundesweite Ausschreibung eine zuverlässige IT-Sicherheitslösung. Die Entscheidung fiel schließlich auf den führenden deutschen Anbieter von IT-Sicherheitstechnologie Rohde & Schwarz Cybersecurity sowie den deutschen Hersteller und Dienstleister im Bereich der Übertragungstechnologie Pan Dacom Direkt GmbH.

Sozialversicherungsdaten enthalten höchst private Informationen, die nicht in unberechtigte Hände geraten dürfen. Gerade bei der elektronischen Übertragung muss jederzeit die Vertraulichkeit und Integrität zum Schutz der Daten gewährleistet sein.

Darauf legt auch der Verband der Ersatzkassen – Interessenverband und Dienstleistungsunternehmen aller Ersatzkassen in Deutschland – höchsten Wert. „Wir sehen uns in der Pflicht, stets die sichersten Verschlüsselungstechniken einzusetzen, um auch für die Zukunft einen zweifelsfreien Schutz der uns anvertrauten Daten garantieren zu können", erklärt Peter Neuhausen, Abteilungsleiter IT des Verbandes. Der vdek trägt die Verantwortung für Dienstleistungen, die eine reibungsfreie, bundesweite Versorgung von 26 Millionen Versicherten der Ersatzkassen unterstützen.

Zur Sicherstellung der Verfügbarkeit der immer größer werdenden Datenmengen hat der vdek unter anderem ein sogenanntes Remote-Backup in einem externen Datenzentrum eingerichtet. Dieses ist mehrere Kilometer von der Zentrale entfernt und über bestehende öffentliche Glasfaserverbindungen kostengünstig angebunden. Dies erfordert aber spezielle Schutzmaßnahmen: „Sensible Daten dürfen nicht unverschlüsselt über öffentlichen Grund und Boden übertragen werden", unterstreicht der Experte des vdek. „Die Gefahr eines unautorisierten Zugriffs wäre einfach zu hoch."

Anforderungen: schnell, sicher, effizient

Neben dem größtmöglichen Schutz ihrer Daten sind für die Mitgliedskassen des vdek auch ein hoher Datendurchsatz und ein rasches Agieren auf sich ändernde Anforderungen wichtig. „Eine schnelle, effiziente

und sichere Verschlüsselungslösung ist elementar für uns, um Massendaten in kürzester Zeit verarbeiten und bereitstellen zu können", sagt Neuhausen.

Für die Entscheidung zwischen den Bewerbern der bundesweiten Ausschreibung waren darüber hinaus eine BSI-Zulassung, hohe Verfügbarkeit und Service entscheidend. Um ein späteres aufwändiges und teures Nachrüsten zu vermeiden, sollte die Lösung bereits jetzt eine synchrone Spiegelung der Daten ermöglichen. Entscheidender Faktor hierfür war eine hohe Bandbreite bei gleichzeitig geringer Latenz.

Diese Anforderungen konnte technologisch nur die R&S SITLine ETH-Produktfamilie der Rohde & Schwarz Cybersecurity GmbH erfüllen, die die Ausschreibung zusammen mit ihrem etablierten Integrationspartner, der Pan Dacom Direkt GmbH, gewann und damit zukünftig Sozialversicherungsdaten zwischen den Rechenzentren schützt. Die Pan Dacom Direkt GmbH, einer der führenden Produktentwickler und Produktintegratoren im Bereich der Übertragungstechnik, übernimmt vom Einbau der Hardware-Lösungen über den Anschluss an die bereits bestehenden Glasfaserleitungen bis zur Betreuung vor Ort ebenfalls die Funktion des direkten Ansprechpartners für die systemorientierte Lösung. „Gerade für große Rechenzentren ist die Lösung von Rohde & Schwarz Cybersecurity perfekt geeignet", erklärt Yurda Oktay, Leiterin Geschäftsentwicklung der Pan Dacom Direkt GmbH. „Sie bietet höchstes technisches Niveau und ist zugleich einfach zu integrieren."

Problemlose Integration

Die Sicherung des Datenverkehrs mit Verschlüsselern der R&S®SITLine-Gerätefamilie ist mit wenig Aufwand verbunden: Außer den Sicherheitsparametern sind keine weiteren netzwerkspezifischen Konfigurationen erforderlich. Sicherheitsmanagement und Netzwerkmanagement sind voneinander getrennt, sodass R&S®SITLine-Geräte problemlos in bestehende IT-Systeme integriert werden können. Dadurch entfällt eine aufwendige Anpassung der Netzwerkinfrastruktur.

R&S®SITLine-Verschlüsseler sind aber nicht nur bei Punkt-zu-Punkt-Verbindungen oder Sternstrukturen einsetzbar. Durch die innovative Gruppenverschlüsselung kann auch die Übertragung in vollvermaschten „switched networks" effizient abgesichert werden. Verbände und Unternehmen können so Speicherlösungen ungefährdet auf mehrere geografisch entfernte Standorte verteilen. Dabei spielt es sicherheitstechnisch keine Rolle, ob sie zur Vernetzung gemietete oder eigene Leitungen einsetzen. Ein weiterer Pluspunkt: Die Netzwerkverschlüsseler von Rohde & Schwarz Cybersecurity sind vom BSI für die Verarbeitung von Daten der Vertraulichkeitsgrade VS-NfD und NATO Restricted zugelassen. Gesetzliche Vorschriften zum Schutz personenbezogener Daten werden damit hundertprozentig eingehalten. „Als IT-Sicherheitspartner der Bundesregierung erfüllt Rohde & Schwarz Cybersecurity nicht nur unsere technischen Anforderungen", ergänzt Peter Neuhausen. „Wir schätzen auch die Vertrauenswürdigkeit deutscher IT-Sicherheitsprodukte."

Mitlesen verhindern

Zur Absicherung der Sozialversicherungsdaten kommt konkret der Ethernet-Verschlüsseler R&S®SITLine ETH40G zum Einsatz, der über das zentrale Sicherheitsmanagement SITScope einfach und intuitiv eingerichtet und administriert wird. Der R&S®SITLine ETH40G wurde speziell für den verschlüsselten Austausch riesiger Datenmengen in Echtzeit entwickelt, wie sie in Rechenzentren verwendet werden. Durch die bislang weltweit einmalige Durchsatzrate von 40 Gigabit/s bei nur 3 Mikrosekunden Latenz für die Verschlüsselung erfüllt das neue Flaggschiff aus der R&S®SITLine ETH-Gerätefamilie die anspruchsvollen Anforderungen im Rechenzentrumseinsatz – und das bei einem Platzbedarf von nur einer Höheneinheit. Zum technischen Hintergrund: Die Verschlüsselung erfolgt bereits auf der sogenannten Sicherungsschicht (Layer 2), was einen zusätzlichen Vorteil bringt: Der Security-Overhead gegenüber IP-Verschlüsselung (Layer 3) ist um bis zu 40 Prozent reduziert – das spart Bandbreite. Damit ist die Geräteklasse für den vdek ideal: Sie bietet Schutz in öffentlichen Netzen, ohne Abstriche bei deren Leistungsfähigkeit zu machen.

Der R&S®SITLine ETH40G setzt auf der von Rohde & Schwarz Cybersecurity eigenentwickelten Plattform-Architektur auf. Diese modulare Hard- und Software-Architektur bündelt die Vorteile von hochsicheren Individualentwicklungen und kostengünstigeren Standardlösungen für die Netzwerk-Kommunikationssicherung.

Made in Germany

Als 100-prozentige Tochter des familiengeführten Elektronikkonzerns Rohde & Schwarz entwickelt und produziert Rohde & Schwarz Cybersecurity in Deutschland. Das hat zwei Vorteile: Zum einen ist so eine schnelle und langfristige Verfügbarkeit der Plattformkomponenten und der darauf basierenden Produkte gewährleistet. Zum anderen können sich Kunden auf die hohen deutschen Datenschutzstandards verlassen – ein wichtiger Pluspunkt, vor allem beim Einsatz von Verschlüsselungstechnik. Mit der Pan Dacom Direkt GmbH als Produktintegrator hat sich der Verband der Ersatzkassen e.V. gleichfalls für ein deutsches Unternehmen mit eigener Entwicklungsabteilung und Produktion in Deutschland entschieden.

Kontakt:
Esther Ecke,
Tel.: +49 (0)234 610071 212,
Fax: +49 (0)234 610071 5212,
E-Mail: e.ecke@sirrix.com

Firmen-Hauptsitz von BeeWaTec in Pfullingen – hier arbeiten das Vertriebsteam und die Mitarbeiter der Konstruktion.

Lückenloser Know-how-Schutz für BeeWaTec

Um sein Know-how vor Datenverlust und Datendiebstahl zu schützen, benötigte der Hersteller von Betriebseinrichtungen und Intralogistik-Lösungen BeeWaTec eine Lösung für Data Leak Prevention (DLP). Die Wahl fiel auf Endpoint Protector 4.0 von CoSoSys, da die Software granulare Einstellmöglichkeiten für die Überwachung aller Schnittstellen zulässt und mit einer durchdachten Oberfläche die Bedienung einfach macht.

Immer wieder ist zu lesen, dass mittelständische Unternehmen den Wert ihrer Daten unterschätzen und daher den Schutz vor ungewollter Herausgabe vernachlässigen. Nicht so die BeeWaTec GmbH mit Sitz in Pfullingen. Sie ist spezialisiert auf Lösungen für die innerbetriebliche Logistik und stellt Montage-Arbeitsplätze, fahrerlose Transportsysteme für die bedarfsgerechte Bereitstellung von Produktionsmaterial und Baukastensysteme für Produktionshilfsmittel wie Regale und Wagen her. Zudem bietet BeeWaTec mit dem Produktbereich „Basics" alles, was moderne Firmen für Büro-, Betriebs- und Lagereinrichtungen benötigen. Mit diesen Lösungen sorgt der Anbieter in Werkstätten und den Werkshallen produzierender Unternehmen in ganz Europa für effizientes Arbeiten. Da das Unternehmen die Systeme selbst entwickelt und optimiert und den Aufbau von Montagelinien und Lagersystemen kundenspezifisch plant, stellen Konstruktionszeichnungen, Baupläne und Kundendaten das entscheidende Know-how und damit das wichtigste Kapital dar. Um diese Daten vor ungewolltem Abfluss zu schützen, werden bereits seit Jahren die USB-Schnittstellen der PCs blockiert. Gleichzeitig wird so verhindert, dass Schadcode über Speichersticks ins Firmennetz gelangt.

Immer mehr potenzielle Lecks

„Dann wurden als Reaktion auf die wachsende Gefahr von ungewolltem Datenverlust strengere Sicherheitsrichtlinien eingeführt und weitere Schnittstellen blockiert", sagt Jennifer Konrad, IT-Administratorin bei BeeWaTec und zusammen mit einem Kollegen verantwortlich für Netzwerk, Storage, Backup und Datenbanken an insgesamt sieben Standorten in Deutschland und den Nachbarländern. Es zeichnete sich jedoch schnell ab, dass die bestehende Lösung den gestiegenen Anforderungen nicht gewachsen war. „Da die Mitarbeiter mit Kunden und Partnern Daten austauschen müssen und dafür beispielsweise FTP und unterschiedliche Portale nutzen, mussten immer mehr Freigaben eingetragen werden, um die Arbeitsabläufe nicht zu beeinträchtigen", erläutert sie. „Allerdings konnten die Freigaben jeweils nur für alle Devices oder Schnittstellen erteilt und nicht auf einzelne Abteilungen, Gruppen oder Nutzer heruntergebrochen werden." Bald wies der Schutz vor ungewolltem Datenverlust mehr Löcher auf als ein Emmentaler Käse.

Policies bis auf User-Ebene herunterbrechen

Die Lücken wollte BeeWaTec mit einer neuen DLP-Lösung schließen. „Die Hauptanforderungen waren, dass sie jede Art von Schnittstellen, ob physisch oder nicht, an den Endpoints überwachen kann und granulare Einstellmöglichkeiten bis auf User-Ebene bietet", sagt die Administratorin. „Auch die Thin Clients, die wir neben den PCs im Unternehmensnetz einsetzen, sollte die neue Lösung überwachen." Weiterhin war die Anbindung an das Active Directory erforderlich. Für eine möglichst einfache Bedienung sollte die Lösung einer Logik folgen, die sich ohne langwierige Schulung oder Beschäftigung mit dem Handbuch erschließt. Bei einer Internetrecherche stieß Jennifer Konrad auf Endpoint Protector von CoSoSys und nahm die Software neben den Produkten anderer Hersteller in die engere Wahl.

Geht doch: technisch komplex und einfach zu bedienen

In einer Testumgebung konnten die Favoriten zeigen, welches Funktionsspektrum tatsächlich in ihnen steckt und wie sie sich handhaben lassen. „Endpoint Protector gefiel uns sehr, weil die Lösung von der

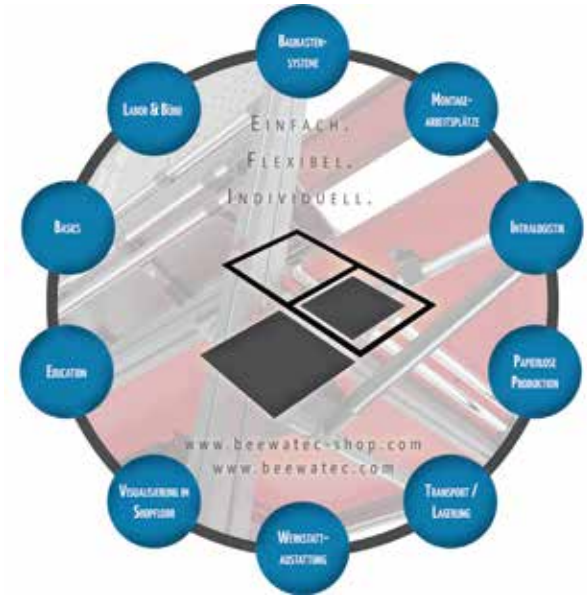
Funktionalität her sehr komplex ist und uns dadurch große Flexibilität bei den Einstellmöglichkeiten der Policies gibt", beschreibt Konrad ihre Eindrücke aus der Vorab-Installation. „Gleichzeitig erschien uns die Benutzeroberfläche sehr übersichtlich aufgebaut, wir konnten sie vom ersten Moment an intuitiv bedienen und die dahinterliegende Logik leicht nachvollziehen." Weitere Pluspunkte sammelte Endpoint Protector mit der zentralen webbasierten Oberfläche für Administration und Reporting und dem im Vergleich zu anderen Lösungen sehr guten Preis-/ Leistungs-Verhältnis.

Zusatzschutz durch Zwangsverschlüsselung

BeeWaTec entschied sich daher für Endpoint Protector und erwarb 170 Lizenzen für die PCs und Thin Clients. Eingesetzt werden die Module Device Control und Content Aware Protection, das Dateien vor dem Transfer über browserbasierte Schnittstellen auf sensible Inhalte prüft, sowie die Verschlüsselungslösung EasyLock. „Wir hatten ursprünglich nicht damit gerechnet, dass Zwangsverschlüsselung als eine Funktion von Gerätekontrolle verfügbar ist und über dieselbe Oberfläche wie die anderen Module bedient werden kann", sagt Konrad. Sie begründet den Erwerb der Zusatzfunktion mit der höheren Sicherheit, den EasyLock für die Daten bietet, die die Mitarbeiter auf USB-Sticks zu den Kunden mitnehmen. Bei Bedarf könnte die IT-Administration mittels eines Unternehmenszertifikates sogar unterbinden, dass die Mitarbeiter Firmendaten auf ihren privaten Rechnern zur Weiterbearbeitung speichern, wo sie sich außerhalb der Kontrolle des Unternehmens befinden und für Wirtschaftsspione leichtere Beute sein können als im Unternehmen.

Einführung Schritt für Schritt

Konrad und ihr Kollege nutzen Endpoint Protector als virtuelle Appliance und haben das Image auf XenServer installiert. Die Basis-Installation einschließlich des Rollouts der Agenten auf die Clients und die Definition der Gruppen dauerten länger als eigentlich erforderlich, die Einführung der Lösung ist noch nicht in Gänze abgeschlossen. „Das liegt an unserer Arbeitsweise. Wir haben uns entschieden, Endpoint Protector nicht auf einen Schlag, sondern etappenweise einzurichten, immer wenn das Tagesgeschäft uns Zeit lässt", sagt Konrad. „Dafür eignet sich die Lösung wegen ihres Aufbaus einfach perfekt."



BeeWaTec ist spezialisiert auf Lösungen für die innerbetriebliche Logistik und Systeme für Büro-, Betriebs- und Lagereinrichtungen.

Mehr Sicherheit mit wenigen Mausklicks

Mit dem Handling von Endpoint Protector und den bisher installierten Funktionen ist sie sehr zufrieden. So wurden als erster Schritt die Policies technisch umgesetzt, die schnell zu mehr Sicherheit führen, die Überwachung der USB-Ports. Nicht jeder Mitarbeiter muss Unternehmensdaten auf USB-Sticks ziehen, die Nutzung der Speichermedien wird an allen Rechnern blockiert. Ausnahmen werden für diejenigen eingerichtet, die Unterlagen auf USB-Sticks beim Kunden präsentieren. An diesen Endpoints lassen sich nur genehmigte Devices anschließen; die Mitarbeiter können keine USB-Sticks benutzen, die sie von zuhause mitbringen oder geschenkt bekommen. Das hat den Effekt, dass Malwarebefall und Spionageangriffe per BadUSB verhindert werden. Die Verschlüsselungskomponente sorgt dafür, dass die Daten auf Sticks, die eventuell unterwegs abhandenkommen, durch Unbefugte nicht einsehbar sind.

BeeWaTec hat sich für Endpoint Protector 4 als virtuelle Appliance entschieden.

Exzellenter Support

Die Umsetzung weiterer Policies kommt an die Reihe, sobald die Administratoren Zeit dafür finden. „Einmal eingerichtet, benötigt die Lösung keine Administration und stellt für unser knappes Zeitbudget keine zusätzliche Belastung dar", freut sich Konrad. „Nur wenn USB-Sticks und Endgeräte neu hinzukommen, müssen wir tätig werden, aber das ist im Handumdrehen erledigt." Die Logfiles liest sie nach Bedarf aus.

Auch die Zusammenarbeit mit Endpoint Protector ließ kaum etwas zu wünschen übrig. Auf Fragen und die Unklarheiten der beiden Administratoren, die sich bei der Einrichtung ergaben, habe der Support unmittelbar reagiert und Hinweise für schnelle Lösungen gegeben. Ihre Vorschläge für Verbesserungen hat der Hersteller aufgegriffen und ist bereits dabei, sie technisch umzusetzen. Mit einem der kommenden Produkt-Updates werden sie allen Kunden zur Verfügung stehen.

BeeWaTec GmbH
Kunstmühlestraße 16
D-72793 Pfullingen
Tel.: +49 (0) 7121-62 87 16-0
info@beewatec.de
www.beewatec.de

Endpoint Protector GmbH
Gebhardstraße 7
88046 Friedrichshafen
Tel.: +49 7541 978267 30
info@endpointprotector.de
www.endpointprotector.de

Film ab! Kaspersky schützt IT bei Kinopolis

Auf der Leinwand sind im Kinopolis die großen Stars zu sehen. Hinter den Kulissen spielt die neue IT-Sicherheitslösung die Hauptrolle.

Mit einer über 100-jährigen Unternehmensgeschichte gehört die Kinopolis-Gruppe zu den traditionsreichsten deutschen Kinobetrieben. Das in Darmstadt ansässige Familienunternehmen bietet heute den Kinobesuchern an bundesweit 17 Standorten, auf insgesamt 137 Leinwänden und mit 27.537 Sitzplätzen viele Möglichkeiten für spannende und unterhaltsame Filmerlebnisse. Zu den größten Standorten zählen der Mathäser Filmpalast in München und die Kinopolis-Niederlassungen im Main-Taunus-Zentrum, in Landshut und Viernheim.

Im Dezember 2013 eröffnete das Unternehmen in Gießen das jüngste Kino der Gruppe. Der Komplex umfasst neun Säle mit insgesamt 1.461 Plätzen, wovon ein Saal mit dem neuen Dolby-Atmos-Tonsystem ausgestattet ist.

Als einer der größten Kinobetreiber Deutschlands ist es für die Kinopolis Management Multiplex GmbH entscheidend, eine zuverlässige IT-Sicherheitslösung einzusetzen. Diese soll das Unternehmen umfassend schützen – vor den zunehmenden Bedrohungen im World Wide Web, beispielsweise in Form manipulierter Webseiten oder schädlicher Mail-Anhänge, aber auch vor Risiken durch infizierte Datenträger wie USB-Sticks.

Denn auch wenn Viren, Trojaner und sonstige Schadsoftware glücklicherweise bisher einen Bogen um die IT-Landschaft der Kinokette gemacht haben, ist Cyberkriminalität ein ernstgenommenes Thema in den IT-Abteilungen.

Gutes Zusammenspiel von IT und Security

Die bisher eingesetzte IT-Security-Lösung konnte die Anforderungen der stark gewachsenen IT-Infrastruktur in der Kinopolis-Gruppe nicht mehr erfüllen. Deshalb suchten die IT-Verantwortlichen nach einer Alternative mit größerem Funktionsumfang. Diese sollte zum einen den Administratoren mittels einer anwenderfreundlichen Konsole die bessere Verwaltung der Softwarelizenzen ermöglichen und ihnen zum anderen ein übersichtlicheres Reporting liefern.

Weitere Kriterien waren, dass die Prozesse bei der Administration reibungslos ablaufen und die Endpoints und Netzwerkkomponenten, welche durch die Lösung geschützt werden, auch künftig performant bleiben. Außerdem sollte der IT-Schutz auch auf Rechnern eingesetzt werden können, auf denen noch Windows 2000 installiert ist. Auch Kompatibilitätsprobleme mit anderen Softwareprodukten aus der IT-Architektur galt es auszuschließen. Die Empfehlung des IT-Security-Dienstleisters choin! GmbH gab den Anlass, die Lösungen von Kaspersky Lab auf den Prüfstand zu stellen.

IT-Schutz ohne Performance-Einbuße

Zur Auswahl standen schließlich zwei Anbieter, die mit ihrem Lösungsportfolio auch komplexe IT-Strukturen bedienen können. Ausschlusskriterium bei einem der Anbieter war jedoch die Tatsache, dass der IT-Schutz zu Lasten der Performance und Ressourcenkapazitäten zu gehen drohte.

Dies war bei Kaspersky Lab nicht der Fall. Auch die sonstigen gestellten Anforderungen konnten erfüllt werden. Somit war die Entscheidung für den Security-Spezialisten aus Ingolstadt schnell getroffen.

Schnelle und einfache Implementierung

Im Zeitraum von April bis Juli 2013 wurde schließlich in der Kinopolis Management Multiplex GmbH die bisherige IT-Sicherheitslösung gegen Kaspersky Endpoint Security for Business Advanced European Edition ausgetauscht. Da der Kino-Spezialist über eine sternförmige IT-Topologie verfügt, wurde bei der Implementierung der Kaspersky-Software zuerst das Kaspersky Security Center in der Darmstädter Zentrale ins-

talliert. Von dort aus fand der schrittweise Rollout der Lösung auf die Server und Clients an den jeweiligen Standorten statt. Im Laufe dieses Projekts hat Kinopolis gute Beziehungen zu dem Team des Security-Dienstleisters choin! aufbauen können.

Die gesamte Implementierung konnte weitgehend selbstständig durch die IT-Mitarbeiter bei Kinopolis durchgeführt werden. Offene Punkte konnten schnell mit den Technikern von choin! geklärt werden. Nach einer Woche waren die Einarbeitungszeit für die Administration und die Schulung der Anwender abgeschlossen. Insgesamt schützt Kaspersky Endpoint Security for Business Advanced heute 50 Server und ca. 550 Clients.

Rundum besser geschützt mit Kaspersky

„Mit Kaspersky Lab haben wir in Sachen IT-Security einen großen Schritt nach vorne gemacht", erklärt Robert Ritzi, IT-Systemkaufmann bei der Kinopolis Management Multiplex GmbH. „Unsere IT-Systeme sind nun besser geschützt – und das ohne nennenswerten Performanceverlust. Updates laufen im Hintergrund ab, so dass unsere Mitarbeiter ungestört arbeiten können."

Die Kinopolis-Mitarbeiter werden durch den neuen Viren-Schutz nicht beeinträchtigt, da die Aktualisierung der Signatur-Datenbanken automatisch startet, sobald auf dem Kaspersky-Server neue Updates vorliegen. Auch die Bereinigung der IT-Systeme erfolgt automatisch, falls der Viren-Scanner Schadprogramme entdeckt. Robert Ritzi bringt es auf den Punkt: „Unsere IT arbeitet weiterhin stabil und ist jetzt besser geschützt – was will man mehr."

Kaspersky Labs GmbH
Despag-Straße 3
85055 Ingolstadt
Deutschland
info@kaspersky.de
www.kaspersky.de

KASPERSKY lab

Kinopolis in Zahlen & Fakten

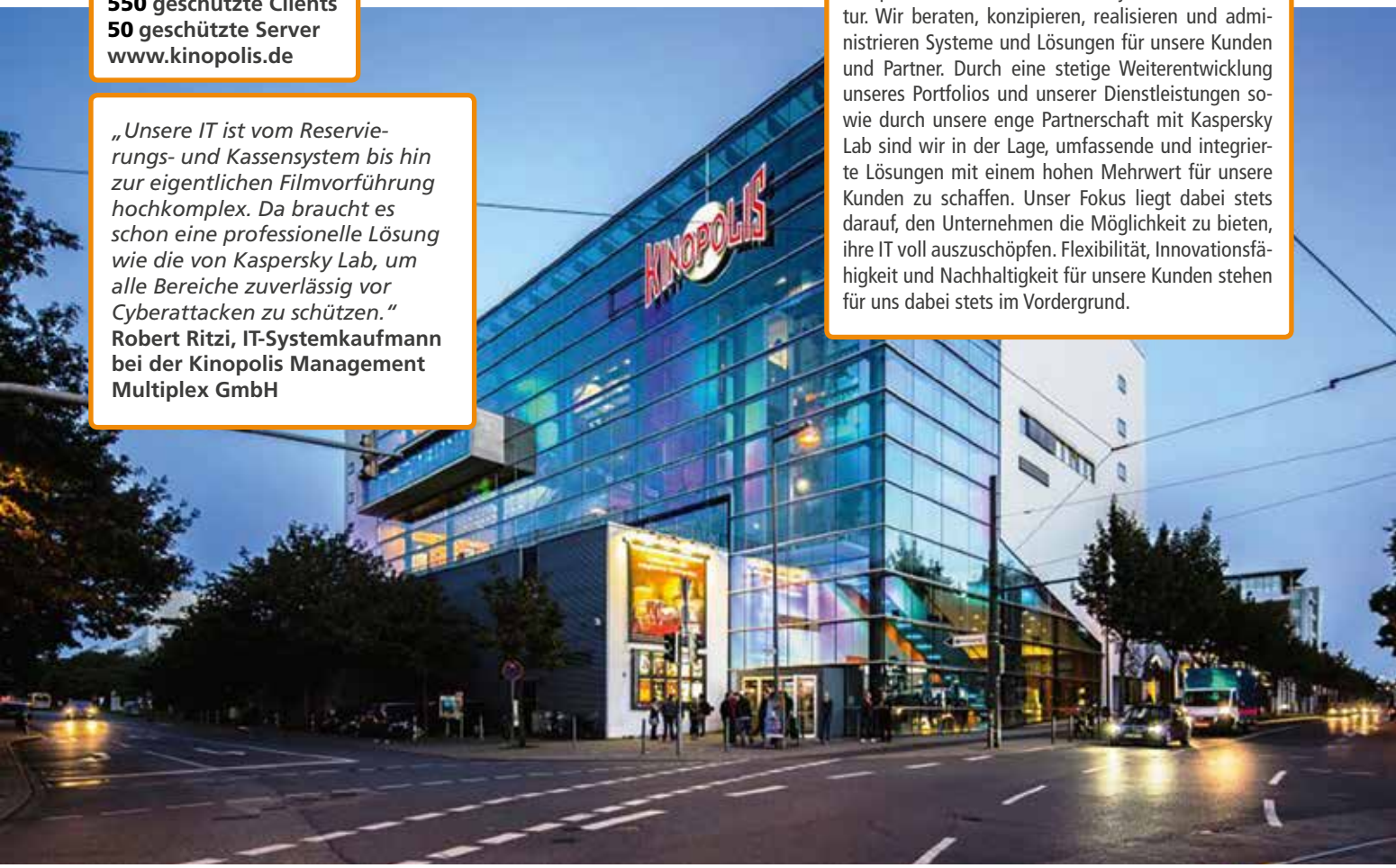
1.000 Mitarbeiter
137 Leinwände
27.537 Sitzplätze
550 geschützte Clients
50 geschützte Server
www.kinopolis.de

„Unsere IT ist vom Reservierungs- und Kassensystem bis hin zur eigentlichen Filmvorführung hochkomplex. Da braucht es schon eine professionelle Lösung wie die von Kaspersky Lab, um alle Bereiche zuverlässig vor Cyberattacken zu schützen."
Robert Ritzi, IT-Systemkaufmann bei der Kinopolis Management Multiplex GmbH

Über choin!

choin! the way IT works

Die choin! GmbH unterstützt Unternehmen seit 2002 als Spezialist im Bereich IT-Security und IT-Infrastruktur. Wir beraten, konzipieren, realisieren und administrieren Systeme und Lösungen für unsere Kunden und Partner. Durch eine stetige Weiterentwicklung unseres Portfolios und unserer Dienstleistungen sowie durch unsere enge Partnerschaft mit Kaspersky Lab sind wir in der Lage, umfassende und integrierte Lösungen mit einem hohen Mehrwert für unsere Kunden zu schaffen. Unser Fokus liegt dabei stets darauf, den Unternehmen die Möglichkeit zu bieten, ihre IT voll auszuschöpfen. Flexibilität, Innovationsfähigkeit und Nachhaltigkeit für unsere Kunden stehen für uns dabei stets im Vordergrund.



Am besten landen Daten im Schredder – sichere Zerstörung von digitalen Datenträgern als Chance für Entsorger

Wenn neue Rechner ins Haus kommen, müssen Unternehmen oft in Tausenden alter Computer vielfach sensible Daten sicher löschen – eine zeitaufwendige Sache. Dank des Festplattenvernichters HDS 230 von HSM kann die Uriel Papierrohstoffe GmbH in Diez (Limburg) ihren Kunden eine schnelle und absolut sichere Datenlöschung anbieten: die mechanische Zerstörung der Festplatten in viele Partikel.

Andreas Uriel, Inhaber der Uriel Papierrohstoffe GmbH, hat eigentlich nichts gegen technische Datenblätter zur Leistungsfähigkeit einer Maschine. Doch was sie tatsächlich kann, probiert er gern selbst aus. Der Firmenchef und diplomierte Kaufmann ist ein zupackender Mann. Also fütterte er für ein paar Stunden den HSM-Schredder mit PC-Festplatten. Und siehe da: 8 Stück pro Minute oder 480 pro Stunde sind möglich – statt der angegebenen 6 pro Minute (oder 360 pro Stunde). Für den Firmenchef ist das eine wichtige Erkenntnis: „Wir können nicht absehen, welche Mengen künftig auf uns zukommen", sagt er. Da ist es gut zu wissen, dass der HSM-Festplattenvernichter Reserven hat.

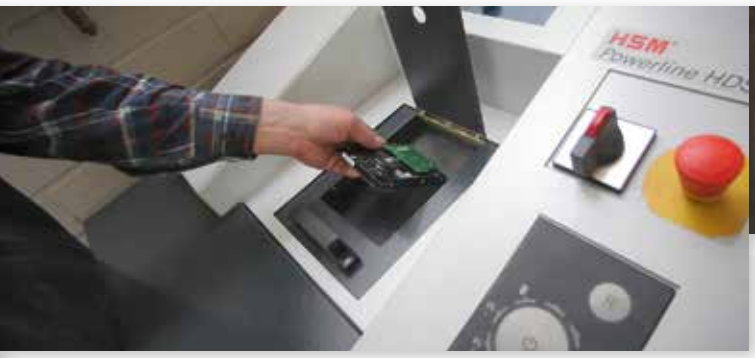
Der Festplattenvernichter hat noch Reserven

Wie der Firmenname Uriel Papierrohstoffe sagt, beschäftigt sich der Entsorgungsspezialist eigentlich mit dem Erfassen, Sortieren und Vermarkten von Wertstoffen. Rund zwei Drittel des jährlich anfallenden Entsorgungsvolumens von 120.000 Tonnen sind Papier und Kartonagen (Verpackungsmaterial). Mit der sicheren Entsorgung von optischen und magnetischen Datenträgern in Form von Festplatten betritt das Unternehmen Neuland: „Das machen wir auf Wunsch bestimmter Kunden." so Andreas Uriel. Zur Kundschaft des Entsorgungsunternehmens im Bereich Akten- und Datenträgervernichtung gehören Banken und Steuerberatungsunternehmen ebenso wie Ärzte, Krankenhäuser oder Software- und IT-Unternehmen. Sie müssen nicht nur alte Rechner entsorgen, sondern Sorge dafür tragen, dass besonders sensible und vertrauliche sowie personenbezogene Daten" geschützt werden, auch wenn die Rechner ausrangiert werden. So will es das Bundesdatenschutzgesetz (BDSG). Als „sensibel" gelten digitale Patientenakten, Bankdaten oder Steuerunterlagen sowie geheime, für Unternehmen wichtige Informationen wie Patente, Konstruktionsunterlagen, Verträge oder Strategiepapiere.

Die mechanische Zerstörung ist die sicherste Methode

Nun ist das Sammeln von Daten angesichts wachsender Speicherkapazitäten der Festplatten bei gleichzeitig sinkenden Preisen kein großes Problem. Schwerer ist ihre sichere Löschung. Zwar gibt es dafür spezielle Software-Programme. Sie überschreiben die Datenspeicher viele Male, um die Informationen unlesbar und nicht wiederherstellbar zu machen. Doch das ist sehr zeitaufwendig, wie man sich bei Hunderten oder gar Tausenden von Unternehmensrechnern leicht vorstellen kann. Wie es schneller geht, beschreibt Andreas Uriel so: „Der sicherste und effektivste Weg ist die mechanische Zerstörung des Datenträgers."

Was das Entsorgungsunternehmen dabei zu beachten hat, legt die neue DIN 66399 fest, die seit Oktober 2012 gilt. Sie beschreibt anhand von drei Schutzklassen und sieben Sicherheitsstufen, wie besonders „sensible Daten" zu vernichten sind und welche Anforderungen die dafür eingesetzten Maschinen erfüllen müssen. Für die Sicherheitsstufe H-4 müssen sie Festplatten in Partikel von maximal 2000 mm² zerkleinern. Der HSM-Festplattenvernichter schafft deutlich mehr: Die Partikel sind viel kleiner als gefordert – ca. 1000 mm². Das Granulat liefert das Unternehmen an Schrotthändler, die das Aluminium in der Festplatte von den übrigen Teilen trennen. Die übrigen Teile werden an Kupferhütten



oder Scheideanstalten weiter verkauft. Denn in den Festplatten sind Edelmetalle wie Kupfer, Gold, Silber oder Platin enthalten, dessen Rückgewinnung sich lohnt.

Ausgereifte Schredder-Technologie

Seit der HSM-Festplattenvernichter bei dem Entsorgungsspezialisten im Einsatz ist, hat Andreas Uriel ein paar Sorgen weniger. Denn bis dahin fehlte es an leistungsfähigen Schreddern. „Wir haben es eine Weile mit Kunststoff- und Papierschreddern versucht", sagt der Firmenchef. Doch für die Metallteile in der Festplatte erwiesen sich die Schneidwerkzeuge als zu schwach. Die Folgen beschreibt Andreas Uriel so: „Wir hatten einen enormen Verschleiß und wegen häufiger Reparaturen lange Stillstandzeiten." Für den neuen Festplattenschredder wurde Andreas Uriel bei HSM in Frickingen fündig. Dem Spezialisten für Entsorgungstechnologien eilt nicht nur ein guter Ruf voraus, was die Qualität seiner Schredder und Ballenpressen betrifft. Für Andreas Uriel war auch wichtig, dass die „Maschinen im Alltag erprobt sind, die Technologie also ausgereift ist".

Hoher Sicherheitsaufwand

Seit rund zwei Jahren ist der HSM-Festplattenvernichter bei Uriel Recycling im Einsatz. Aktuell ist das Gerät nicht ausgelastet. Dennoch ist sich Firmenchef Andreas Uriel sicher, dass sich die Anschaffung als lohnende Investition erweist. Er ist davon überzeugt, dass bei Uriel Recycling bald sehr viele Festplatten zur Vernichtung anstehen: „Die eigentliche Konjunktur steht noch aus." Der Grund für seine Zuversicht: Die Solid State Drive (SSD) wird langfristig die herkömmliche Festplatte verdrängen. „Dann freuen wir uns auf die vielen Festplatten", sagt Andreas Uriel, „die sicher entsorgt werden müssen."

HSM GmbH + Co. KG
Austraße 1-9
88699 Frickingen
Tel. +49 7554 2100-0
Fax +49 7554 2100-160
info@hsm.eu • www.hsm.eu

Die Fakten

Unternehmen

Die Uriel Papierrohstoffe GmbH in Diez (Limburg) ist ein typisches mittelständisches Unternehmen der Entsorgungswirtschaft. Die 1949 von Gerhard Uriel gegründete Firma führt heute sein Sohn Andreas. Der Entsorgungsspezialist sammelt und bereitet vor allem Altpapier, Kunststoffe, Metalle und Holz, aber auch gemischte Gewerbeabfälle bis hin zu Sonderabfällen für die Wiederverwertung auf. Das jährliche Volumen liegt bei 120.000 Tonnen. Auf Wunsch vieler Kunden bietet Uriel seit einiger Zeit auch die sichere Vernichtung von elektronischen Datenträgern wie Festplatten, CDs, DVDs oder Flash-Speicherkarten an.

Aufgabe

Auf den Festplatten ausrangierter Rechner von Banken, Steuerberatern, Krankenhäusern etc. sind Unmengen an persönlichen Daten oder geheimen Unternehmensinformationen wie Patente, Konstruktionsunterlagen und Strategiepapiere gespeichert. Diese „besonders sensiblen und vertraulichen sowie personenbezogenen Daten" müssen laut dem Bundesdatenschutzgesetz (BDSG) geschützt werden. Dazu gehört auch die sichere Löschung oder Vernichtung. Wie optische und magnetische Datenträger vernichtet werden müssen und welche Anforderungen Maschinen zur Vernichtung der verschiedenen Datenträgerarten erfüllen müssen, legt die DIN 66399 fest. Sie ist seit Oktober 2012 in Kraft. Als sicherster und effektivster Weg gilt die mechanische Zerstörung des Datenträgers.

Lösung

Für die Vernichtung von Datenträgern nutzte Uriel Papierrohstoffe lange Zeit Schredder, die ursprünglich für Papier und Kunststoffe gedacht waren. Mit der steigenden Menge an Festplatten nahm auch der Verschleiß an den Schreddern zu. Sie standen oft wegen Reparaturen still. Außerdem waren sie nicht nach der DIN-Norm zertifiziert, die festlegt, in welche Partikelgröße optische und magnetische Datenträger (DVDs, Festplatten, etc.) zerteilt werden müssen. Deshalb schaffte Uriel Papierrohstoffe den HSM-Festplattenvernichter HDS 230 an.

Nutzen

- Hoher Durchsatz: Dank der speziellen Schneidwerkzeuge des HSM-Festplattenvernichters können mehr als 400 Festplatten pro Stunde zerkleinert werden
- Recycling: Das Aluminium in der Festplatte sowie Edelmetalle wie Gold, Silber und Platin sind begehrte Rohstoffe
- Hohe Zuverlässigkeit: Der Festplattenvernichter läuft zuverlässig, kein Stillstand
- Schneller Service: Wenn Probleme auftreten, sind die Techniker von HSM schnell mit passenden Ersatzteilen vor Ort
- Leichtes Einarbeiten neuer Mitarbeiter: Der Festplattenvernichter ist einfach zu bedienen
- Return on Investment (ROI): Geschätzt circa 1 bis 3 Jahre (je nach Marktpreis für Metallteile aus Festplatten)

Besuchen Sie die Fachtagung zum Thema Datenschutz!

41. DAFTA 2017 16.–17. November 2017 in Köln

mit dem 36. RDV-Forum am 15. November 2017

im Maternushaus Köln

Perspektiven des Datenschutzrechts 2018 – Anforderungen und Praxis

- Rund 350 Teilnehmer informieren sich auf 9 verschiedenen Parallelforen rund um die Themen Datenschutz und Datensicherheit
- Top-Referenten führen durch Fachvorträge und spannende Diskussionsrunden
- Aussteller präsentieren ihre Lösungen und Tools für die Datenschutzpraxis
- Veranstaltung mit Tradition: Die DAFTA ist eine der größten Fachtagungen zum Thema Datenschutz in Europa
- Fortbildungsveranstaltung gemäß § 4f Abs. 3 BDSG/Art. 38 DS-GVO
- In 10 Vortragsmodulen informieren Sie unsere Experten über Aktuelles im Umfeld von Datenschutz und Informationssicherheit. Seien auch Sie dabei!

Jetzt informieren und anmelden unter www.dafta.de

GDD-Winter-Workshop

Für Datenschutzbeauftragte und -berater sowie Datenschutzdienstleister

29.–30. JANUAR 2018

in Garmisch-Partenkirchen

— Bitte beachten Sie unser Seminarangebot unter www.datakontext.com —

Sichern Sie sich Ihren fachlichen Vorsprung!

DATAKONTEXT

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT GmbH · Augustinusstr. 9d · 50226 Frechen · Telefon 02234/98949-40 · Telefax 02234/98949-44 · www.datakontext.com · tagungen@datakontext.com