

Web Security für kommunales Rechenzentrum

Sensibler Webfilter: Pflicht wird zur Kür

Mit Blick auf seine Kunden hat sich das Kommunale Rechenzentrum Minden-Ravensberg/Lippe für eine mandantenfähige Web Security Lösung entschieden.

1200 Mitarbeiterinnen und Mitarbeiter des Kommunalen Rechenzentrums Minden-Ravensberg/Lippe (krz) in Lemgo und bei seinen Kunden werden bei ihren Zugriffen auf das Internet mit Hilfe von Websense Web Security zuverlässig vor unerwünschten Angriffen geschützt.

„Für das krz war die Einführung dieses Content-Filters eine wichtige Pflichtmaßnahme“, sagt Karl-Ernst Blübaum, Geschäftsbereichsleiter Kommunikationstechnik beim krz, einem Zweckverband, der seine Mitglieder – die Kreise Minden-Lübbecke, Herford und Lippe sowie 34 Städte und Gemeinden aus diesen Kreisgebieten – als Informatik-Dienstleister umfassend betreut. Vorgeschrieben sei diese Sicherheitsmaßnahme zwar nicht explizit, aber um sich effektiv vor den vielfältigen Varianten von Malware zu schützen, kommt man ohne Webfilter nicht mehr aus. Daran liegt Blübaum umso mehr, als das krz das erste BSI-zertifizierte öffentlich-rechtliche Rechenzentrum in Deutschland war.

Ob Informationsrecherchen oder die Nutzung von Softwareanwendungen über das Web, „das Internet ist längst ein unverzichtbares Arbeitsmittel für alle Mitarbeiterinnen und Mitarbeiter der öffentlichen Hand“. Deshalb muss bei der Webnutzung für einen ausreichenden Schutz gesorgt werden. Und die Anforderungen an die Websicherheit – und zwar sowohl an die Konzepte, als auch an die technischen Lösungen – sind groß angesichts der Professionalisierung bei Schadsoftware und Hackerszene.

„Die Lösung kann nur in einem Maßnahmenbündel bestehen“, sagt Karl-Ernst Blübaum. „Neben Virenscannern am einzelnen Arbeitsplatz sind URL-Filter als zentraler Ansatz zusammen mit Firewall und Proxy eine wichtige Komponente.“

Dienstvereinbarung zum privaten Surfen

Am Beginn des Weges zur Einführung von Websense Web Security im krz in Lemgo standen u.a. eine Kundenanfrage sowie eine Dienstvereinbarung im kommunalen Rechenzentrum, die das private Surfen verbot. In der Folge wurden stichprobenartige Kontrollen durchgeführt. „Den Kollegen gleichsam hinterher zu schnüffeln ist natürlich unangenehm“, sagt Blübaum. Eine Web Security Lösung erspart dies. Diese bot sich zudem deshalb an, weil das krz auch minderjährige Auszubildende hat, die es schützen muss.

Eine Selbstverständlichkeit war die Einführung des Content-Filters dennoch nicht, zumal das krz eine Lösung zusammen mit seinen Mitgliedern anstrebte, die gleichzeitig seine Kunden sind. Eine Maßnahme, die nicht eindeutig vorgeschrieben ist, die Geld kostet, ohne dass der Vorteil sehr konkret greifbar oder gar mit harten Zahlen bezifferbar ist, war gegenüber den öffentlichen Verwaltungen angesichts stets knapper Kassen schwer zu argumentieren.

Letztlich entschied sich das krz zur Vorreiterrolle und schlug dafür einen Weg ein, auf dem sich seine Kunden jederzeit einbinden können, erläutert Blübaum. Mandantenfähigkeit war folglich eine der wichtigsten Anforderungen an die zu findende Softwarelösung. Gesucht wurde eine schlanke Webfilterlösung mit hoher Qualität der Ergebnisse, die in die Infrastruktur des krz passte.

Seit Jahren wird das krz bereits vom IT-Security Dienstleister AMPEG aus Bremen betreut. „Deshalb war AMPEG auch gleich unser unmittelbarer Ansprechpartner, als wir nach einer Lösung suchten“, so Blübaum. Gemeinsam wurde die Web Security Lösung von Websense ausgewählt. Nach einem erfolgreichen Test wurde die Lösung Anfang 2008 in Betrieb genommen.



Systematische Zugriffsverhinderung

„Websicherheit bedeutet nicht nur einfaches URL-Blocken“, sagt Gerhard Langer, Senior Consulting Engineer bei AMPEG. „Viel mehr geht es darum, das Netzwerk vor den Gefahren aus dem Internet zu schützen.“

Spyware, Keylogger oder Trojaner werden durch den Missbrauch des Internet in rasender Geschwindigkeit weltweit verteilt. „Die systematische Verhinderung von Zugriffen auf potenziell gefährliche Seiten ist somit zum Standard geworden“, sagt Langer. Um den ständig neuen oder sich verändernden Gefahren entgegen zu wirken, ist ein Einsatz von Reputationsfiltern unumgänglich. Die Sicherheitsanbieter haben sich auf die Gefahren längst eingestellt. Bei Websense werden die Reputationsbewertungen stündlich an über zwei Millionen Domains, Netzwerke, IP-Adressen und Hosts übergeben. Somit ist es möglich, sich dem schnell verändernden Internet anzupassen. Mittels des eigenen ThreatSeeker-Netzwerks werden zudem stündlich 40 Millionen Webseiten auf entstandene Bedrohungen überprüft.

„Die Trefferwahrscheinlichkeit von Websense, mit der Webseiten korrekt beurteilt werden, ist hoch“, betont Blübaum. Schließlich soll zwar die Gefährdung der Daten – ob durch menschliches Versagen oder bösartige Angriffe von außen – möglichst ausgeschlossen werden. Die Produktivität der Mitarbeiterinnen und Mitarbeiter dürfe aber zugleich nicht eingeschränkt werden, etwa durch unberechtigtes Blockieren von Seiten.

Das krz hostet die Content-Lösung

Die seit Anfang 2008 eingesetzte Websense-Lösung des krz nutzen heute auch der Kreis Minden-Lübbecke und die Stadt Preußisch Oldendorf. Das krz hostet das Produkt, ansonsten agieren die Administratoren der Verwaltungen selbständig, vor allem stellen sie ihr eigenes Regelwerk für die Nutzung auf und machen das Reporting für ihre Kommune. Voraussetzung ist die Mandantenfähigkeit von Websense Web Security, zu deren Optimierung das krz seinen Teil beitrug.

Anfangs konnte nämlich stets nur ein Administrator zu einem bestimmten Zeitpunkt zugreifen – bei steigender Nutzerzahl wäre das eine große Hürde geworden. Zusammen mit dem Kreis Minden-Lübbecke wies daher das krz den Hersteller in einem Workshop nachdrücklich auf diesen Mangel hin. Heute sind zeitgleich lokale und zentrale Zugriffe auf Websense problemlos möglich. „Die hohen Anforderungen, die das krz an die Mandantenfähigkeit der Software stellt, sind sicherlich eine kommunale Besonderheit“, sagt Blübaum.

Eine deutliche Vereinfachung brachte zudem die einheitliche Weboberfläche für die Administration: Das heißt nicht nur das Reporting, sondern auch die Produktverwaltung erfolgen über die Browseroberfläche. Das Berichtswesen als wichtiger Bestandteil des Produkts enthält vordefinierte Berichte, beispielsweise welche Gruppen am meisten Bandbreite belegen, wie viele Zugriffe auf das Web getätigt bzw. verweigert wurden. Erfasst wird ebenso, welche Nutzer am meisten Sperrungen hatten und welche Sites dies vorrangig betraf oder die Aktivität der wichtigsten fünf Benutzer auf den Seiten Online-Shopping, Unterhaltung und Sport.

Datenschutz sicherstellen, Personalrat einbinden

Hier zeigt sich sehr deutlich, dass bei der Einführung einer Lösung wie Websense Web Security aus Datenschutzgründen der Betriebs- bzw. Personalrat eingebunden werden muss, auch wenn dies natürlich Zeit kostet. „Zumal“, wie Blübaum erläutert, „mit solch einem Tool auch leistungsbezogene Auswertungen möglich wären: Beispielsweise könnte eine Liste der User, die am meisten im Internet unterwegs waren, überprüft werden auf die Frage hin, ob die besuchten Seiten tatsächlich arbeitsrelevant waren.“

Letztlich war die Zustimmung des Personalrats zur Einführung eines Content-Filters unvermeidbar, obwohl das krz das private Internetsurfen untersagt hatte. Den Umfang der Kontrollen und die zulässigen Auswertungen hat das krz zusammen mit dem Personalrat im Detail in einer Dienstvereinbarung geregelt.

Erfreulich sind auch funktionale Verbesserungen, die die Version 7 gebracht hat. Eine Toolbox auf der Eingangsoberfläche beispielsweise erlaubt es sehr schnell zu überprüfen, zu welcher Kategorie eine eingeschränkte URL gehört, ob diese Kategorie künftig vielleicht freigegeben werden kann oder aber welche Richtlinie für welchen Client gilt. Auf diese Weise kann mit wenig Zeitaufwand beständig das Berechtigungskonzept geprüft und aktualisiert werden.

„Einen Unterschied zwischen öffentlicher Hand und Privatwirtschaft gibt es in Sachen Websicherheit keine“, sagt AMPEG-Berater Gerhard Langer. Sowohl die Bedrohungslage als auch die rechtlichen Rahmenbedingungen sind die gleichen, die technische Infrastruktur sei ähnlich, und auch das Problembewusstsein in gleicher Weise gemischt. „Während in großen Einheiten meist Sicherheitsbeauftragte entsprechend der Vorschriften das Thema vorantreiben, warten kleine Einheiten meist, bis etwas Gravierenderes passiert ist“, so Langer. Um erfolgreich zu sein, muss die technische Websicherheitslösung in jedem Fall in eine verwaltungs- oder firmenweite Sicherheitspolitik integriert werden.

Meilensteine auf dem Weg zur Websicherheit

ab 2006:	erste Überlegungen, Produktauswahl, Testinstallationen
Mitte 2007:	Einbeziehung des Personalrats, Echtttest
Nov. 2007:	Entscheidung für Websense als Web Security Lösung im krz mit der Option, krz-Kunden (Verwaltungen) zu integrieren
Januar 2008:	Produktivbetrieb für das krz
Februar 2009:	Produktivbetrieb für zwei weitere Verwaltungen

Resümee

„Die Einführung von Websense hat ganz klar einen Beitrag zur Sicherheitskultur im krz geleistet“, lautet das Fazit von Karl-Ernst Blübaum. Die Benutzer seien sensibler geworden beim Zugriff auf das Internet und wägen im Wissen um die Kontrollen stärker ab.

Erfreulicherweise bietet Websense aber auch die Flexibilität, quasi eine Grauzone einzurichten, hebt Karl-Ernst Blübaum hervor. Beispielsweise lässt sich für bestimmte Seiten-Kategorien anstelle einer Zugriffsverweigerung ein Warnhinweis einrichten, so dass der Zugriff auf eine bestimmte URL noch einmal bestätigt werden muss. Oder es kann Client-bezogen ein Zeitkontingent pro Tag etwa im Umfang eines Teils der vorgeschriebenen Pausenzeiten vergeben werden, das für die Nutzung eher privater Webseiten eingeräumt wird.

Content-Filter sind nicht explizit vorgeschrieben, dennoch sollten sie Bestandteil eines Websicherheitskonzeptes sein, betont krz-Geschäftsbereichsleiter Blübaum. Würde das krz dafür das selber gewählte Produkt weiterempfehlen? „Als mandantenfähige zentrale Lösung“, sagt Blübaum, „ist Websense Web Security auch für andere Rechenzentren interessant.“ Und mit AMPEG hat das krz einen Partner für das Produkt gewählt, mit dem die Zusammenarbeit sehr fachkompetent, zuverlässig und engagiert ist.

Die Lösung wurde realisiert beim:

KRZ Kommunales Rechenzentrum Minden- Ravensberg/Lippe
Schloßstraße 15
32657 Lemgo

Kontakt

AMPEG Technologie und Computer Service GmbH
Obernstraße 45-47
28195 Bremen
Tel. 0421-525870
Fax 0700-26734329