HORNETSECURITY

WEBFILTER SERVICE

WHITEPAPER

1 Problemstellung Webfilter

1.1 Gründe für den Einsatz von Webfiltern

1.1.1 Abwehr von Bedrohungen der IT-Sicherheit

Webserver sind einer der wichtigsten Angriffswege für Bedrohungen der IT-Sicherheit von Unternehmen. Über infizierte Websites schleusen Angreifer Schadcode auf die Systeme von Nutzern, spähen Logindaten oder andere persönliche Benutzerdaten aus oder greifen darüber direkt auf Daten auf dem System des Nutzers zu. Unterscheiden lassen sich zwei Arten von Angriffen: Solche, bei denen der Angreifer gezielt den Aufruf der schädlichen Website provoziert („Push") und solche, bei denen der Nutzer eher zufällig auf eine kompromittierte Website stößt („Pull").

Bei Push-Angriffen werden mehrere Angriffswege kombiniert eingesetzt (sog. „Blended Attacks"). Der Angriff beginnt z.B. durch eine Welle ausgesandter Spam-Nachrichten, in denen der Link auf die schädliche Website enthalten ist. Idealerweise filtert der Spamfilter derlei Nachrichten aus. Angreifer versuchen aber naturgemäß ihre Absichten zu verschleiern. Deshalb werden die so versandten Nachrichten nicht nur in Inhalt und Aufmachung immer geschickter, sondern die enthaltenen Links verweisen anfangs oft auf harmlose Webseiten. Als Folge erkennen viele Spamfilter die Nachrichten nicht oder erst mit Verzögerung als Spam. Deshalb landen viele dieser Nachrichten trotz Spamfilter im Postfach des Empfängers.

Wenn der Empfänger die Nachricht einige Zeit später öffnet, ist die bisher harmlose Webseite durch eine schädliche Webseite ersetzt. Der Nutzer wird durch Inhalt und Aufmachung der Nachricht zum Klick auf den Link animiert („Ihre EC-Karte wurde gesperrt. Klicken Sie hier für weitere Informationen!") und der Schaden ist angerichtet. Auch gezielt platzierte Links in Blogs und Social Sites dienen dazu, Nutzer auf schädliche Webseiten zu lenken.
Bei Pull-Angriffen werden normale, an sich harmlose Websites von Hackern gezielt infiziert. Die Websites werden so manipuliert, dass Benutzer der Site unbeabsichtigt und für sie nicht feststellbar Schadcode (z. B. Trojaner, Root-Kit) laden, auf ihrem System installieren und ausführen (sog. „Drive-by Downloads"). Nach einer Untersuchung von WhiteHat Security weisen 44% aller Webserver permanent Sicherheitslöcher auf, weitere 26% sind zeitweise unsicher. Schätzungen zufolge sind mehrere hunderttausend bis eine Million Websites durch Ausnutzung dieser Sicherheitslöcher tatsächlich kompromittiert.

Die in den meisten Unternehmen im Netzwerk installierten Firewalls und in Client-Systemen installierten Antivirus-Programme sind zwar notwendig, können aber keinen effektiven Schutz gegen den Angriffsweg über Webserver bieten. Webfilter schützen vor diesen Angriffen durch Sperre der betroffenen Websites und Analyse der von Websites geladenen Daten auf Schadcode und ergänzen dadurch die Schutzmaßnahmen sinnvoll.

1.1.2 Erfüllung rechtlicher Anforderungen[1]

Welche rechtlichen Verpflichtungen Unternehmen gegenüber ihren Mitarbeitern im Hinblick auf den Schutz des Webverkehrs haben, hängt zunächst stark davon ab, ob das Unternehmen die private Nutzung des Internets zulässt oder nicht. Ist private Internet-Nutzung erlaubt oder geduldet, gilt das Unternehmen als Diensteanbieter im Sinne des Telemediengesetzes – mit weitreichenden Folgen und Verpflichtungen. So verbietet z. B. § 88 des Telekommunikationsgesetzes jegliche Überwachung des Internetverkehrs. Die Sperre bestimmter Websites kann entsprechend § 85 als unerlaubte Leistungseinstellung betrachtet werden.

In der Regel ist Unternehmen daher ein Verbot der privaten Internetnutzung durch Mitarbeiter zu empfehlen. Sollen Internetzugänge des Unternehmens dennoch für private Zwecke genutzt werden, so sollte die private Nutzung unbedingt im Rahmen einer Betriebsvereinbarung geregelt werden, in der auch auf Art und Umfang von Kontrolle und Eingriffen des Unternehmens in den Internetverkehr, z. B. durch einen Webfilter, hingewiesen wird. Ohne eine solche Regelung ist lediglich der Schutz vor Störungen des Betriebs erlaubt, etwa durch Virusscanner oder das Blocken von als gefährlich eingestuften Websites durch einen Webfilter.

Fehlt eine konkrete Regelung zur Internetnutzung, kann sich daraus auch ein Haftungsrisiko für Unternehmen ergeben. Das Unternehmen haftet nämlich in erster Linie für Verstöße, die mit Hilfe des Internet-Anschlusses des Unternehmens begangen werden (sog. „Störerhaftung"). Beispiele für solche Verstöße sind illegale Downloads von urheberrechtlich geschützten Daten, z. B. Musikdateien oder Computerprogramme. Unternehmen müssen die Internetnutzung nicht nur konkret regeln, sondern durch technische und organisatorische Maßnahmen die Regelungen auch durchsetzen und dazu die Einhaltung der Regeln zumindest stichprobenartig überwachen. Ein Webfilter unterstützt dies durch Sperren entsprechender Inhalte und statistische Auswertung des Webverkehrs.

Ist die private Internetnutzung verboten, sind sehr viel weitreichendere Maßnahmen möglich. Das Unternehmen gilt dann nicht als Dienstanbieter. Es ist von einer rein betrieblichen Nutzung auszugehen und verschiedene gesetzliche Regelungen, wie Telekommunikationsgesetz und Telemediengesetz, sind nicht anwendbar. Zu beachten ist aber, dass auch hier das Verbot nicht nur eindeutig ausgesprochen sondern auch durchgesetzt werden muss. Bei der Durchsetzung kann wiederum ein Webfilter gute Dienste leisten, indem er etwa den Zugriff auf Seiten versperrt, die zur Ausübung der dienstlichen Tätigkeit nicht erforderlich sind.

Unabhängig von erlaubter oder verbotener privater Nutzung bleibt das Datenschutzgesetz anwendbar. Das Bundesdatenschutzgesetz (BDSG) regelt die Erhebung, Verarbeitung und Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer Person, d. h. solche Daten, die einen eindeutigen Personenbezug haben oder für die ein Personenbezug hergestellt werden kann. Personenbezogene Daten im Kontext eines Webfilters können demnach aufgerufene Webseiten sein, deren Inhalte personenbezogene Daten aufweisen. Auch Daten, die den zeitlichen Verlauf des Aufrufs von Webseiten wiedergeben (Weblog), weisen einen klaren Personenbezug auf.
Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nach BDSG außerhalb gesetzlicher Vorschriften nur erlaubt, sofern der Betroffene (Mitarbeiter) eingewilligt hat. Diese Einwilligung ist schriftlich einzuholen. Sie muss außerdem auf der freien Entscheidung des Betroffenen beruhen, d. h.

[1] Die Ausführungen beziehen sich, soweit nicht anders angegeben, auf deutsches Recht.

eine entsprechende Betriebsvereinbarung reicht nicht aus. Vielmehr muss die Vereinbarung mit jedem Betroffenen einzeln getroffen werden und er darf durch eine Verweigerung auch keine gravierenden Nachteile erleiden.

Webfilter sollten deshalb keine personenbezogenen Daten speichern. Soweit personenbezogene Daten verarbeitet oder zwischengespeichert werden, darf dies nur soweit geschehen, wie es zur Übertragung der Inhalte erforderlich ist. Der unbefugte Zugriff auf diese Daten durch Dritte muss durch technische oder organisatorische Maßnahmen ausgeschlossen sein. Lediglich in Einzelfällen, z. B. bei einer festgestellten Störung des Internetbetriebs oder bei festgestelltem, nicht unerheblichen Verstoß gegen betriebliche Regelungen zur Internet-Nutzung (z. B. illegaler Download geschützter Inhalte) dürfen Daten mit Personenbezug zur Feststellung des Störers und Beseitigung der Störung genutzt werden. Webfilter können das unterstützen, indem sie die Aufzeichnung und Auswertung solcher Daten fallweise konfigurierbar machen. Die unbefugte Aktivierung muss allerdings durch besondere Maßnahmen verhindert werden.

Aus der Fürsorgepflicht des Arbeitgebers kann dagegen sogar eine Verpflichtung zur Filterung des Webverkehrs hergeleitet werden. Dies gilt insbesondere für vom Benutzer ungewollte Begleiterscheinungen der Webnutzung, wie Drive-by Downloads oder Phishing-Attacken. Ein Webfilter sollte deshalb den Zugriff auf Seiten mit gefährlichen Inhalten generell sperren oder eine solche Sperre mindestens ermöglichen.

Weitergehend ist die Verpflichtung von Unternehmen zum Schutz minderjähriger Mitarbeiter. Der Jugendmedienschutz-Staatsvertrag (JMStV) verpflichtet Anbieter von Telediensten, dafür zu sorgen, dass Jugendlichen der Zugang zu Angeboten verwehrt wird, die „geeignet sind, die Entwicklung von Jugendlichen zu beeinträchtigen". Daraus lässt sich ableiten, dass Unternehmen verhindern müssen, dass minderjährige Mitarbeiter über betrieblich bereitgestellte Arbeitsmittel Zugang zu jugendgefährdenden Inhalten erhalten, etwa Pornographie oder Gewalt verherrlichenden Inhalten. Dies gilt u. U. auch dann, wenn die private Nutzung des Internets durch das Unternehmen verboten ist, weil in Betracht gezogen werden muss, dass minderjährige Mitarbeiter das Verbot missachten. Auch hier leistet ein Webfilter gute Dienste, indem er für die betroffenen Benutzer den Zugang zu jugendgefährdenden Inhalten blockiert.

1.1.3 Kosten durch privates Surfen am Arbeitsplatz

Nach einer Studie im Auftrag von BITKOM nutzt etwa jeder zweite berufliche Internet-Nutzer während der Arbeitszeit das Web auch für private Zwecke. Manchmal ist eine solche Nutzung durchaus erwünscht, oft geduldet, in vielen Fällen findet sie auch trotz ausdrücklichen Verbots statt. In jedem Fall entstehen dem Unternehmen durch die private Nutzung Kosten durch Nutzung der Infrastruktur des Unternehmens, durch zusätzlichen Datenverkehr und verlorene Arbeitszeit. Die Regelung der privaten Nutzung und die Durchsetzung von Regelungen liegen schon deshalb, auch außerhalb rechtlicher Anforderungen, im Interesse des Unternehmens.

Webfilter unterstützen die Durchsetzung von Nutzungsregeln, indem sie die Blockierung von Websites ermöglichen, deren Nutzung nicht im Interesse des Unternehmens liegt. Soll die private Nutzung eingeschränkt erlaubt sein, können Webfilter die Nutzung bestimmter Websites z. B. in Pausenzeiten erlauben.

1.2 Anforderungen an Webfilter

Aus den Gründen für den Einsatz von Webfiltern lassen sich folgende Anforderungen ableiten:

- Abwehr von Schadcode
  - Sicheres Blockieren potenziell gefährlicher Websites:

    Der Zugriff auf Websites, die bekanntermaßen Schadcode enthalten, in betrügerischer Absicht betrieben werden (z. B. Phishing), klare Rechtsverstöße begehen (z. B. Urheberrechtsverletzungen) oder in anderer Weise unmittelbar die IT-Sicherheit bedrohen (Anonymizer, Hacker-Sites) muss durch den Webfilter blockiert werden.

  - Untersuchung von Datenströmen auf Schadcode:

    Die Datenströme von zugelassenen Verbindungen zu Webservern müssen durch den Webfilter auf Schadcode (Trojaner, Viren etc.) untersucht und ggf. blockiert werden. Auch verschlüsselte Verbindungen (HTTPS) müssen untersucht werden können, dies sollte allerdings je Website konfigurierbar sein. Webfilter sollten auch Datenströme untersuchen, die per FTP übertragen werden.

- Umsetzung von Unternehmensrichtlinien zur Webnutzung
  - Zentral konfigurierbare Richtlinien zur Webnutzung:

    Richtlinien zur Webnutzung sollten im Webfilter nach Kategorien einstellbar sein. Die Einstellung von Richtlinien nach Kategorien ist erheblich einfacher und schneller, als die Einstellung über Black- und Whitelists, in denen verbotene und erlaubte Webserver einzeln eingetragen werden. Die Richtlinien sollten auf Benutzerebene, Gruppenebene und global für das ganze Unternehmen einstellbar sein, um unterschiedliche Richtlinien für unterschiedliche Benutzergruppen zu erlauben und gleichzeitig den Aufwand für die Einstellung der Richtlinien gering zu halten.

  - Sichere Klassifikation von Websites nach Kategorien:

    Die Zahl der weltweit betriebenen Webserver kann exakt nicht benannt werden, es sind auf jeden Fall mehrere hundert Millionen und die Zahl wächst weiterhin rasant. Es gibt keine Datenbank, die alle Websites lückenlos sicher kategorisiert – angesichts des rasanten Wachstums wäre das auch in der Praxis gar nicht möglich. Webfilter müssen deshalb eine möglichst große Zahl der wichtigsten, d. h. meistbesuchten Websites kennen. Wird eine bisher unbekannte Website angefragt, müssen Webfilter über schnelle Mechanismen verfügen, die eine möglichst sichere Kategorisierung ad hoc erlauben. Weiterhin sollte die Kategorisierung einer permanenten Qualitätssicherung unterliegen.

  - Einfacher Freigabeprozess für Ausnahmen:

Die Freigabe einzelner Websites auf Benutzeranfrage sollte einfach und mit wenig Aufwand möglich sein. Auch hier sollten Freigaben auf Benutzerebene, Gruppenebene und unternehmensweit erfolgen können. Idealerweise kann die Freigabe für einzelne Mitarbeiter oder Gruppen von einem benannten Gruppenleiter vorgenommen werden, der die Notwendigkeit einer Freigabe besser einschätzen kann, als ein Systemadministrator. Diese Möglichkeit muss dann aber so einschränkbar sein, dass zwingende Richtlinien (die z. B. der Erfüllung rechtlicher Anforderungen dienen) nicht umgangen werden können.

- Identifikation von Benutzern:

  Der Webfilter muss Benutzer identifizieren können, um die für einen Benutzer geltenden Richtlinien anwenden zu können. Je nach Anforderungen des Unternehmens sollten verschiedene Identifikationsmöglichkeiten zur Verfügung stehen.

- Anbindung mobiler Nutzer:

  Der Webfilter sollte auch Benutzer unterstützen, die von außerhalb des Unternehmensnetzes mit Systemen des Unternehmens im Web surfen.

- Blockieren von Verbindungen außerhalb der Richtlinien:

  Verbindungen, die nach den geltenden und eingestellten Richtlinien für einen Benutzer nicht erlaubt sind, müssen blockiert werden.

- Zeitsteuerung für private Webnutzung in Pausen:

  Sofern das Unternehmen privates Surfen in Pausenzeiten gestattet, sollte der Webserver abweichende Richtlinien für Pausen- und Arbeitszeiten unterstützen.

- Anwendungskontrolle:

  Webfilter sollten den Zugriff bestimmter Anwendungen auf Webserver gezielt zulassen oder verbieten können. Darüber kann die Nutzung bestimmter Browser, von FTP-Clients oder Messenger(z. B. Skype) geregelt werden.
- Informationen und Statistiken zur Webnutzung:

  Zur Durchsetzung von Richtlinien ist Überwachung erforderlich. Ein Webfilter sollte dazu einen Überblick über Art und Umfang genutzter Webservices liefern können. Sofern in Einzelfällen (z. B. bei begründetem Verdacht auf erheblichen Verstoß gegen Richtlinien) eine nutzerbasierte Auswertung erforderlich ist, sollte der Webfilter eine solche Auswertung grundsätzlich ermöglichen.

- Umsetzung von Datenschutzanforderungen

  - Benutzerbasierte Auswertungen:

Benutzerbasierte Auswertungen der Webnutzung sollten nur auf besondere Anforderung möglich und durch gesonderte Maßnahmen geschützt sein.

- Benutzertrennung:

  Daten einzelner Benutzer müssen voneinander getrennt gespeichert werden. Der Zugriff eines Benutzers auf Daten eines anderen Benutzers muss ausgeschlossen sein.

- Technische Anforderungen

  - Durchsatz und Antwortzeiten:

    Eine geringfügige Verlängerung von Antwortzeiten durch einen Webfilter ist in der Regel unvermeidlich. Der Webfilter sollte aber Durchsatz und Antwortzeiten nicht wesentlich verlangsamen.

  - Verfügbarkeit:

    An vielen Arbeitsplätzen sind Mitarbeiter auf die Verfügbarkeit des Webzugriffs angewiesen. Ist kein Webzugriff möglich, ruht die Arbeit oder wird erheblich eingeschränkt. Daher ist für Webfilter eine hohe Verfügbarkeit erforderlich. Bereits eine Verfügbarkeit von 99% bedeutet einen Ausfall von im Mittel 1-2 Arbeitsstunden im Monat. Die Verfügbarkeit sollte deshalb in der Praxis erheblich über 99% liegen. Wartungszeiten sollten nach Möglichkeit vollständig außerhalb normaler Arbeitszeiten liegen, möglichst sollte ein Wartungsfenster durch redundante Infrastruktur nicht zu Ausfällen führen.

2 Webfilter Service

2.1 Cloud Architektur

Cloud Computing wird von Forrester Research definiert als „ein Pool aus abstrakter, hochskalierbarer Infrastruktur mit Anwendungen, die nach Verbrauch abgerechnet werden“. Bildlich kann man sich eine Cloud als eine Wolke von Rechnern vorstellen, die aus der Distanz wie ein homogenes Gebilde wirkt und entsprechend als ein homogenes System behandelt und genutzt werden kann.
Wesentliche Vorteile von Cloud-Computing:

- Dynamische Bereitstellung von Ressourcen nach Bedarf,
- Höhere Verfügbarkeit durch massive Redundanz,
- Keine Installation dedizierter Hard- und Software,
- Hardware- und Betriebssystem-unabhängig,
- Daraus resultierend erheblich flexibler, leistungsfähiger und kostengünstiger als entsprechende dedizierte Infrastrukturen.

Unterschieden wird zwischen verschiedenen Cloud-Typen:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

Ferner gibt es Unterschiede in der Art der Bereitstellung

- Private Clouds – einem für eine Organisation dedizierten Pool von Systemen, der für z. B. verschiedene Anwendungen gemeinsam genutzt wird.
- Public Clouds – Pools von Systemen, die von mehreren Organisationen gemeinsam genutzt werden.
- Hybrid Clouds – eine Mischform von Private und Public Clouds; z. B. Nutzung einer Public Cloud als Ergänzung für eine Private Cloud.
- Community Clouds – im Prinzip eine Private Cloud für eine Gemeinschaft von Nutzern (z. B. Mitglieder eines Verbandes).

Vor allem für Public Clouds gelten zusätzlich zu den allgemeinen Vorteilen von Cloud-Computing folgende Vorteile:

- Keine langfristige Kapitalbindung (OPEX statt CAPEX)
- Keine Installation von Hardware und Software
- Kein oder nur geringer interner Administrationsaufwand

Hornetsecurity nutzt das Prinzip der Public Cloud für seine Managed Security Services, u.a. den Hornetsecurity E-Mail Webfilter Service. Wesentliche Vorteile dieses Ansatzes gegenüber On-Premise Filterung:

- Gemeinsame Nutzung von Hard- und Software durch alle Kunden, dadurch erheblich kostengünstiger als klassische Einzelinstallationen,
- Massiv redundante und verteilte Auslegung des Gesamtsystems, dadurch erheblich leistungsfähiger und robuster als Einzelinstallationen,
- Betrieb außerhalb der Infrastruktur der Unternehmen, dadurch Entlastung der Infrastruktur,
- Betrieb des Systems im Internet, damit grundsätzlich von allen Standorten, Heimarbeitsplätzen und mobilen Nutzern zugänglich (Zugangseinschränkungen sind konfigurierbar),
- 24/7 Überwachung der Systeme durch Security-Experten, dadurch Gewährleistung der Sicherheit und des kontinuierlichen Betriebs auch außerhalb der Arbeitszeiten des eigenen IT-Personals.

Eine Herausforderung für Public Clouds besteht in der Herstellung der Sicherheit und Abgrenzung der Daten verschiedener Nutzer untereinander. Die Lösungen von Hornetsecurity sind deshalb voll mandantenfähig und verfügen über abgestufte Benutzerberechtigungen und ein fein konfigurierbares Berechtigungssystem. Daten werden hierarchisch in separaten Datenbanken je Kunde abgelegt, so dass immer nur der Zugriff auf eigene Daten entsprechend der jeweiligen Nutzer-Hierarchieebene möglich ist.

Die Systeme von Hornetsecurity werden verteilt in verschiedenen gesicherten Rechenzentren betrieben. Generell ist der tatsächliche Ort der Verarbeitung oder Lagerung von Daten nicht auf ein bestimmtes System festgelegt. Trotzdem können bei Hornetsecurity bestimmte Bereiche der Cloud an bestimmte Aufgaben gebunden werden. Für Unternehmen mit Sitz in Deutschland wird entsprechend, soweit

gewünscht, die Filterung des Webverkehrs gemäß Bundesdatenschutzgesetz in Deutschland vertraglich garantiert.

Da, wo es auf Grund großer Datenmengen sinnvoll ist, können Systeme auch in den Rechenzentren von Provider-Partnern und Firmenkunden aufgestellt und betrieben werden – als Hornetsecurity Managed Appliance. Hornetsecurity kombiniert dadurch die Vorteile der Cloud mit denen dedizierter Systeme.

2.2 Aufbau und Funktion

Der Hornetsecurity Webfilter wird primär als Hosted Service angeboten, in größeren Installationen auch als Managed Appliance. Er fungiert als Proxy zwischen den aufrufenden Web-Clients und den aufgerufenen Web-Servern (Abbildung 1).

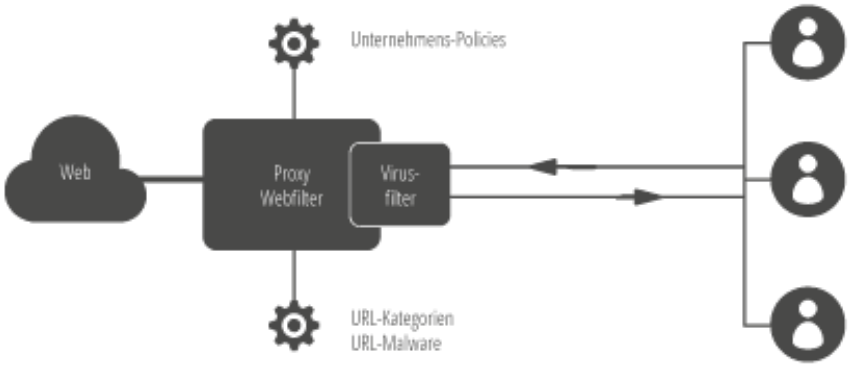

Abbildung 1: Hornetsecurity Webfilter Appliance als Proxy zwischen Client und Webservern

Die Entscheidung, ob einem Benutzer der Zugriff auf Daten erlaubt wird oder nicht, wird im Webfilter mehrstufig getroffen. Ausgewertet werden dazu die eingestellten Richtlinien für den Benutzer und verschiedene URL-Datenbanken. Datenströme werden zusätzlich auf Viren und Malware überprüft.

2.3 Control Panel

Das Control Panel
Abbildung 2) ist der zentrale Zugangspunkt zu allen Informationen und Einstellungen zu Hornetsecurity Services. Es unterstützt Administratoren und Benutzer bei der Verwaltung von benutzerdefinierten Einstellungen, beim Umgang mit Freigabeanforderungen und bei der statistischen Auswertung des Web-Verkehrs. Das umfangreiche Rechtemanagement ermöglicht eine granulare Unterteilung in verschiedene Zugriffsrechte. So können z. B. Helpdesk-Zugänge mit den für Helpdesk-Mitarbeiter notwendigen Rechten angelegt werden.

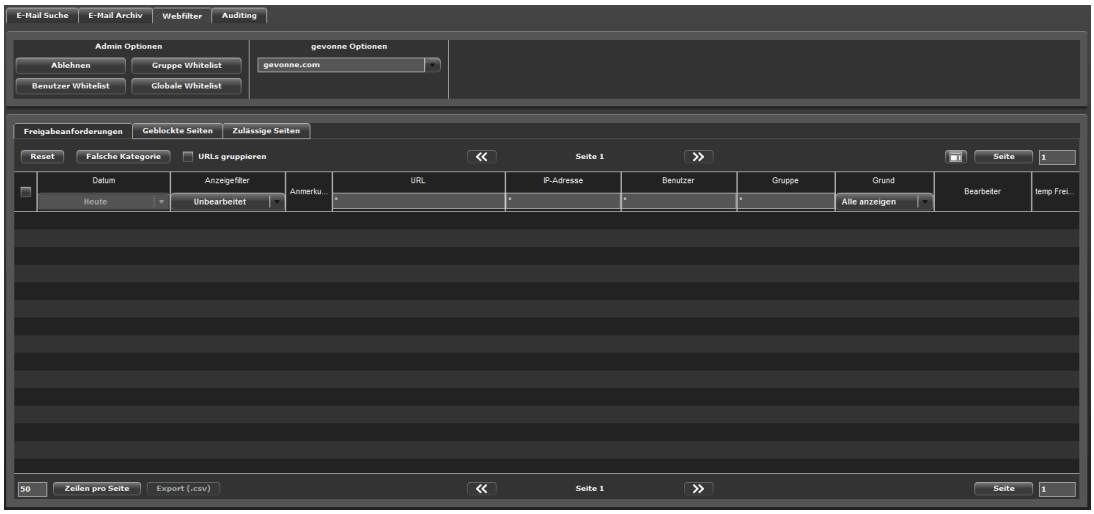

Abbildung 2: Bearbeitung von Freigabeanforderungen im Hornetsecurity Control Panel

Im Control Panel vorgenommene Einstellungen werden automatisch in die Hornetsecurity Cloud übertragen und dort verteilt, typisch nach drei, in Ausnahmefällen spätestens zehn Minuten nach Speicherung arbeiten alle Systeme in der Cloud mit den neuen Einstellungen.

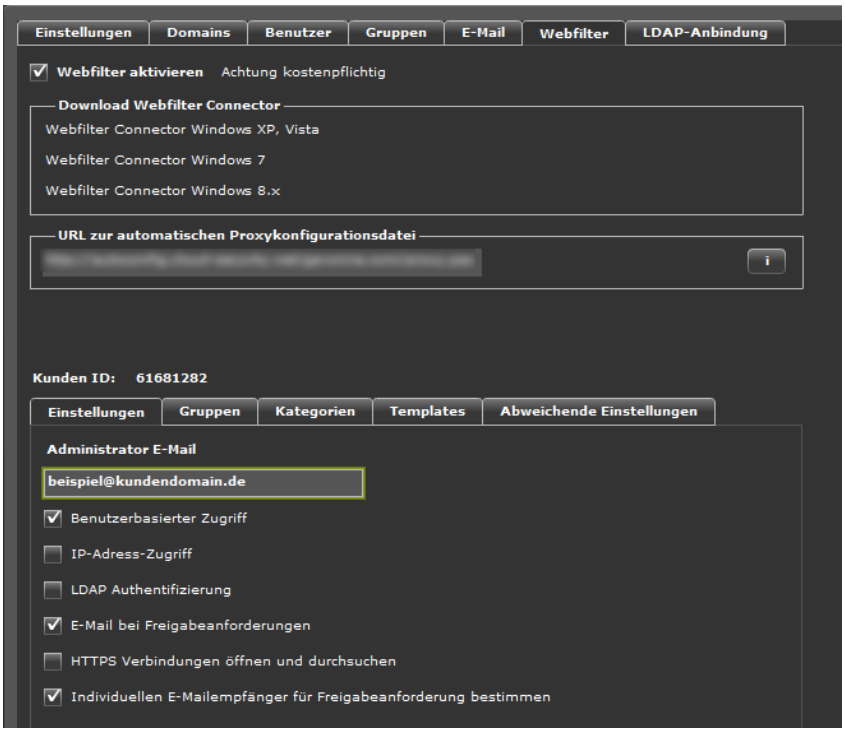

Abbildung 3: Umfangreiche Kontroll- und Konfigurationsmöglichkeiten für Administratoren im Control Panel

Über das Control Panel erfolgt auch die Einrichtung von Benutzern, entweder von Hand, durch Hochladen entsprechender Listen oder durch Abgleich mit einem LDAP-Server. Die Nutzung des Control Panels ist

mit den meisten Browsers mit aktuellem Flash-Plugin möglich. Als webbasierte Anwendung wird das Control Panel automatisch immer in der aktuellsten Version gestartet. So haben alle Nutzer stets Zugriff auf die aktuellsten Features.

Derzeit ist das Control Panel in 17 Sprachen verfügbar: Chinesisch, Deutsch, Dänisch, Englisch, Französisch, Italienisch, Japanisch, Katalanisch, Polnisch, Russisch, Schwedisch, Slowakisch, Spanisch, Ukrainisch, Griechisch, Portugiesisch (PT und BR). Weitere Sprachen sind in kurzer Zeit implementierbar.

2.4 Umsetzung von Unternehmensrichtlinien

Die Sperrung oder Freigabe von Webseiten und Kategorien werden im Hornetsecurity Control Panel über konfigurierbare Policies auf Benutzerebene, Gruppenebene oder systemweit gesteuert. Mit Hilfe der Policies kann das Surfen für bestimmte Kategorien und einzelne Websites auch für festgelegte Zeiten freigegeben werden – außerhalb dieser Zeiten ist der Zugriff auf diesen Websites dann blockiert. Bestehende Black- und Whitelists sind über das Hornetsecurity Control Panel in das System importierbar und werden so Bestandteil der Policies.

Eine umfassende Vorkonfiguration ermöglicht die reibungslose Einführung des Webfilters. Der Aufwand für die Konfigurationen ist minimal, da sich über das zentrale Control Panel die Einstellungen für sämtliche Benutzer an allen Standorten durch Policies vorgeben lassen.

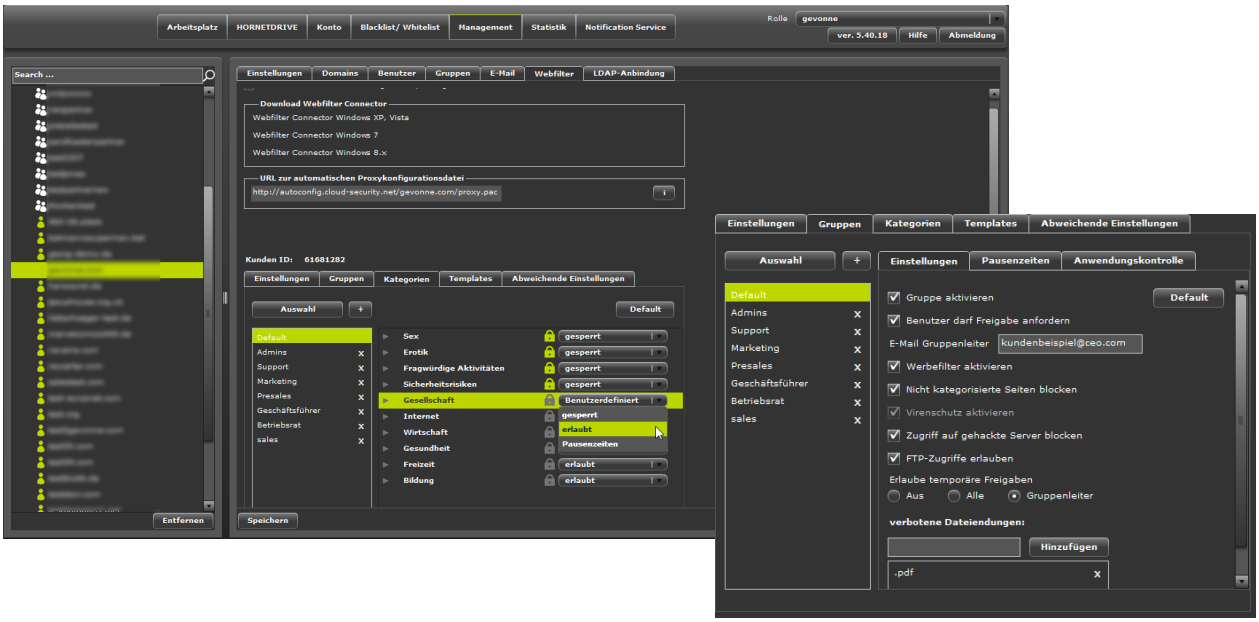

Abbildung 4: Umsetzung von Unternehmensrichtlinien im Hornetsecurity Control Panel

Über das Control Panel können Administratoren auch Änderungen an der Standardrichtlinie für alle Benutzer vornehmen. Die jeweiligen Anforderungen verschiedener Benutzergruppen lassen sich über zusätzlich konfigurierbare Policy-Gruppen steuern, wobei nur die jeweils notwendigen Themenbereiche angepasst werden müssen und alle anderen Berechtigungen vererbt werden (

Abbildung 4).

Mit Hilfe der Policies kann das Surfen für bestimmte Websites auch für festgelegte Zeiten freigegeben werden – außerhalb dieser Zeiten ist der Zugriff auf diese Websites dann blockiert (Abbildung 5).

Ebenfalls einstellbar auf Gruppen- und Systemebene sind erlaubte und verbotene Datentypen bei Downloads. Damit können Downloads auf bestimmte Datentypen (z. B. PDF) eingeschränkt oder gezielt potenziell gefährliche Datentypen (EXE, MSI) verboten werden.

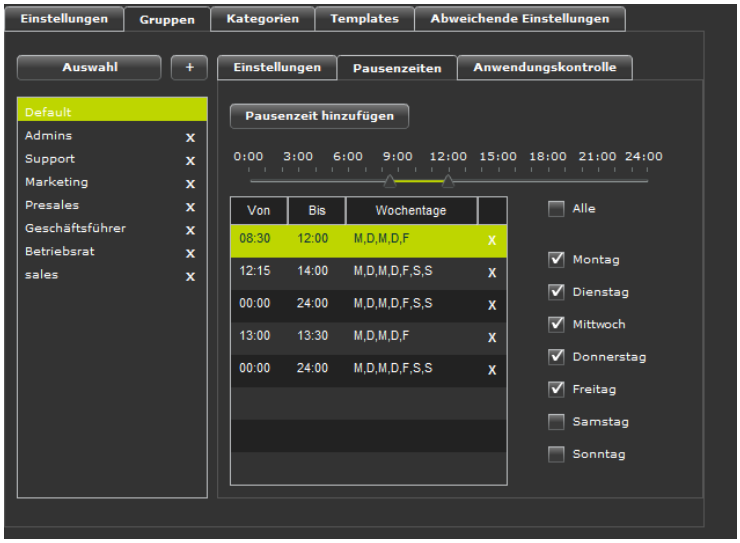

Abbildung 5: Definition von Pausenzeiten

Bei der Sperrung einer Website können Benutzer eine Freischaltung anfordern, die umgehend an den Verantwortlichen gemeldet wird (

Abbildung 6). Anhand der Filterung aller ausstehenden, genehmigten und abgelehnten Anforderungen entsteht eine übersichtliche Liste, die sich mit einem Klick abarbeiten lässt. Das System verschickt anschließend automatisch eine Rückmeldung über den Status der Anfrage. Freigaben einer Webseite können individuell dem anfordernden Benutzer, einer Policy-Gruppe oder pauschal allen Surfenden zugewiesen werden.

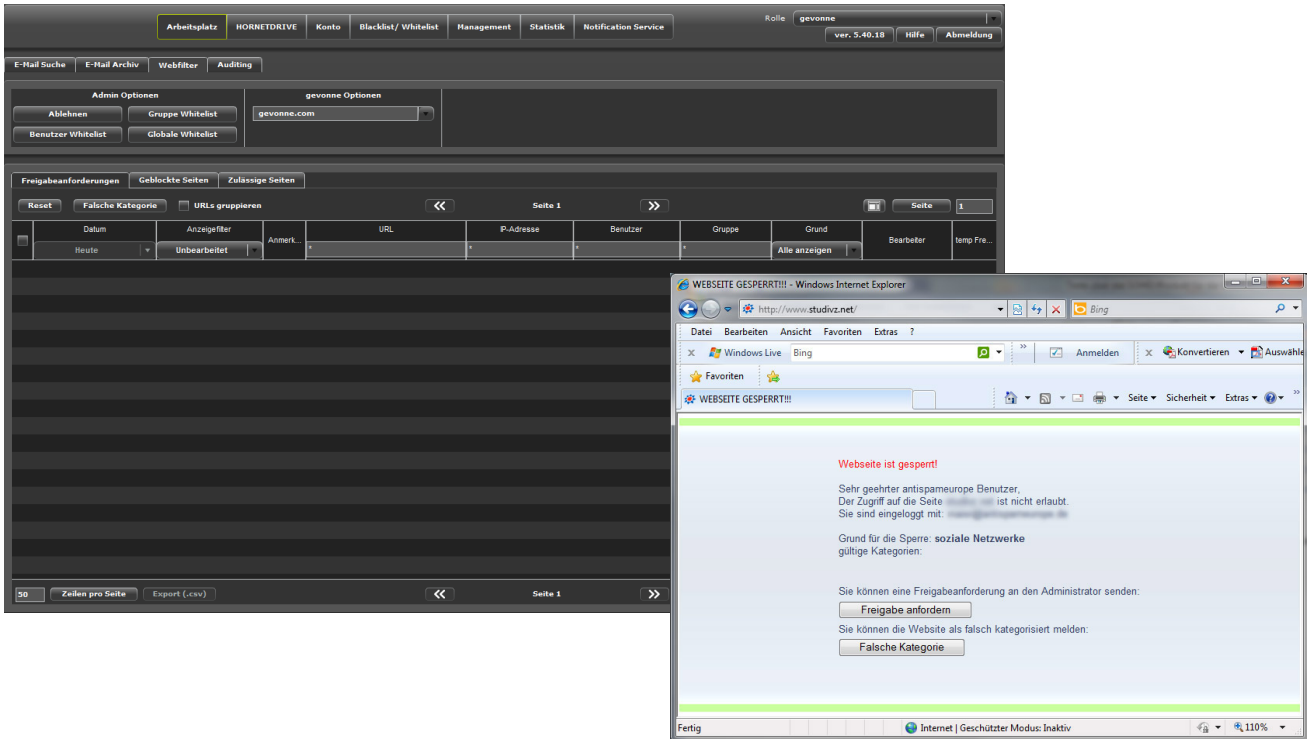

Abbildung 6: Sperre eine Website und Verwaltung von Freigabeanforderungen im Control Panel

Für jede einzelne Gruppe besteht außerdem die Möglichkeit einen Gruppenleiter zu definieren, der Freigabeanforderungen für Websites eigenverantwortlich bearbeiten, d. h. solche Anfragen ablehnen oder bestätigen kann (Abbildung 7).

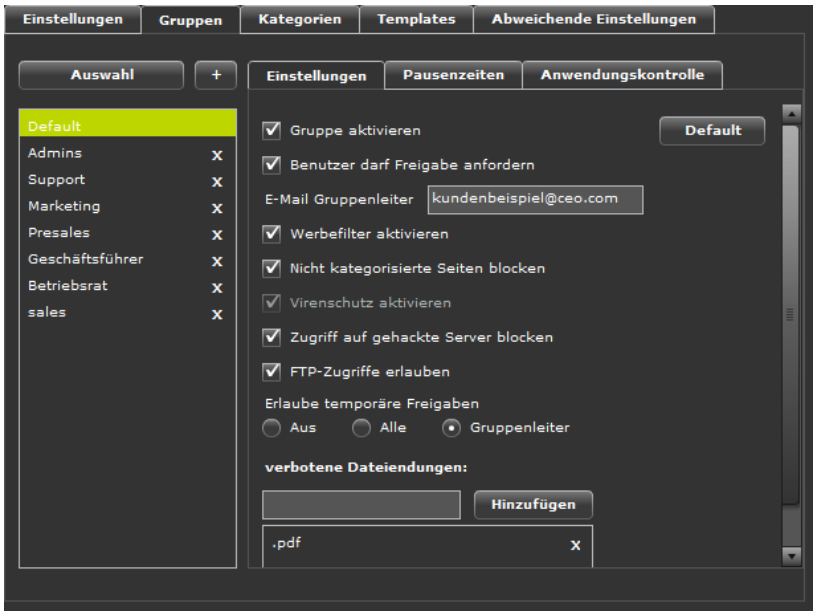

Abbildung 7: Spezielle Gruppeneinstellungen für den Webfilter

Dies ist nützlich, weil Administratoren den Nutzen einer bestimmten Website für eine Abteilung oder Tätigkeit oftmals nicht wirklich einschätzen können. Die Freigabe solcher Websites nimmt der Gruppenleiter ggf. per Link direkt aus der per E-Mail erhaltenen Freigabeanforderung vor.

2.5 Kategorisierung von Webseiten

Webseiten werden vom Hornetsecurity Webfilter an Hand einer Datenbank mit über 450 Millionen klassifizierten Seiten, aufgeteilt in 15 Themenbereichen mit bis zu 18 Unterpunkten (darunter z. B. auch „Gewalt", „Pornographie") kategorisiert. Die Datenbank deckt die Top 1 Million Websites weltweit in 200 Sprachen ab. Eine Nachkategorisierung von in der Datenbank nicht erfassten Websites erfolgt automatisch. Dabei werden folgende Klassifikationsverfahren eingesetzt:

- Inhaltsklassifikation: Sprachanalyse, Inhaltstypen, statistische Textanalyse, heuristische Prüfungen, Script-Analyse, Auswertung von Metadaten

- Erkennung potenziell gefährlicher (malicious) Seiten: Inhaltsscans, Verhaltensanalyse, Reputationsprüfung, Exploit-Erkennung, Malware-Erkennung, Phishing-Erkennung

Zusätzlich erfolgt eine manuelle Nachklassifizierung und Qualitätskontrolle durch ein mehrsprachiges Team (Double Blind Check).

2.6 Virusschutz

Im Hornetsecurity Webfilter ist ein mehrstufiger Virusschutz integriert. Der Virusschutz besteht aus folgenden Komponenten:

1. Blocken von infizierten und kompromittierten Webservern:

Hornetsecurity identifiziert kompromittierte Webserver, CMS-Systeme und Web2.0 Anwendungen sowie offene Webserver, die Schadcode beinhalten oder nachladen. Die Information wird in der Hornetsecurity Reputationsdatenbank in Echtzeit analysiert und aktualisiert.

2. Aktives Scannen von verdächtigen Websites:

Websites werden nach bekannten Sicherheitslücken und Exploits heuristisch überprüft. Hierbei wird speziell darauf geachtet ob Programmcode bekannte Sicherheitslücken in Betriebssystemen und Browsern ausnutzen möchte, sowie die Absicht des auszuführenden Codes überprüft.

3. Untersuchung vom verdächtigem Code im Sandbox-Verfahren:

Um auch bisher unbekannte Sicherheitslücken und Exploits zu erkennen, werden Scripts und Web2.0 Inhalte sowie Software und ausführbarer Code im Sandboxverfahren simuliert, um die Aktivitäten der Software zu analysieren und die Inhalte gegebenenfalls zu sperren.
4. Signaturbasiertes und heuristisches Scannen der Daten im TCP/IP Stream:

Hier werden bekannter und unbekannter Schadcode signaturbasiert und mit heuristischen Verfahren überprüft. Hornetsecurity untersucht dabei nicht nur übertragene Programme (SW-Downloads), sondern kann auch Viren innerhalb TCP/IP Streams feststellen und entsprechend blockieren.

5. Verfolgen von verdächtigen Links

Hornetsecurity überprüft verdächtige Links von vertrauenswürdigen Websites und erkennt Cross-Site-Exploits. Die Informationen werden in den Link-Reputation-Filtern von Hornetsecurity verarbeitet. Zusammen mit den Hornetsecurity Signaturpartnern wird die Datenbank täglich gegen mehrere Milliarden URL-Aufrufe abgeglichen.

2.7 Anbindung von Clients

Der Hornetsecurity Webfilter wird zentral als Proxy betrieben, d. h. die eigentliche Filterung findet zentral statt, nicht auf dem Client. Deshalb muss dafür gesorgt werden, dass Webanfragen über den zentralen Webfilter geleitet werden und nicht direkt und damit ungefiltert erfolgen. Clients können auf folgende Arten an den Webfilter angebunden werden:

- Durch Eintrag des Webfilters als Proxy in den Webbrowser:
  Hornetsecurity stellt dazu eine PAC (Proxy-Auto-Config) Datei zur Verfügung, die im Webbrowser eingetragen wird. Vorteil: Der Webfilter wird von jedem Ort im Internet genutzt – egal ob der Client im LAN oder z. B. im Homeoffice betrieben wird. Nachteil: Je nach Sicherheits-Konfiguration des Clients kann der Benutzer den Proxy unter Umständen deaktivieren und nutzt das Internet dann ungeschützt.

- Durch Umleiten des Datenverkehrs in der Firewall des Firmennetzes:

  Dabei werden durch Regeln in der Firewall alle ausgehenden HTTP (sowie ggf. HTTPS und FTP) Verbindungen auf den Webfilter umgeleitet. Vorteil: Der Webfilter läuft transparent, d. h. eine Änderung der Konfiguration der Clients ist nicht notwendig und Benutzer können den Webfilter auch nicht umgehen. Nachteil: Der Schutz ist nur für Clients innerhalb des Firmennetzes wirksam, Clients außerhalb des Firmennetzes sind nicht geschützt. Werden außerhalb (z. B. im Homeoffice) betriebene Clients allerdings per VPN in das Firmennetz eingebunden, laufen die von diesen Clients ausgehenden Webverbindungen über die Firewall und können entsprechend auch über den Webfilter geleitet werden.

- Durch Eintrag des Webfilters als Standardgateway in den Netzwerkeinstellungen – z. B. über den DHCP-Server. Dadurch wird der gesamte Netzverkehr, der an Adressen außerhalb des internen Netzes gerichtet ist, an den Webfilter weitergeleitet. Vorteil: Auch hier arbeitet der Webfilter transparent. Nachteil: Protokolle, die der Webfilter nicht verarbeiten kann (z. B. SSH, SMTP), werden geblockt und nicht übertragen. Oft ist das durchaus gewünscht, kann aber zu Problemen führen. Deshalb ist die Umleitung des Datenverkehrs durch die Firewall des Firmennetzes die in der Regel gewählte Variante, wenn ein transparenter Betrieb des Webfilters gewünscht wird.

2.8 Authentisierung gegenüber dem Webfilter

Sollen Benutzer- oder gruppenspezifische Web-Policies genutzt werden, ist eine Identifikation des Benutzers durch den Webfilter erforderlich. Der Hornetsecurity Webfilter stellt dazu folgende Mechanismen bereit:

- Manuelle Identifikation durch Eingabe von Benutzername und Kennwort bei Aufforderung durch den Browser:

  Die Benutzerdaten können von vielen Browsern gespeichert werden, was eine wiederholte Eingabe stark vereinfacht. Benutzername und Kennwort können vom Hornetsecurity Webfilter vom LDAP-Dienst des Unternehmens (z. B. Active Directory) übernommen werden.

- Automatische Identifikation durch den Hornetsecurity Connector:

  Der Hornetsecurity Connector ist ein kleines Software-Plugin zur automatischen Identifikation von Benutzern gegenüber dem Hornetsecurity Webfilter. Der Hornetsecurity Connector ist derzeit für folgende Plattformen verfügbar:

  - Windows XP (32 Bit)
  - Windows Vista und Windows 7 (32 und 64 Bit)
  - Windows Server 2003 und 2008 (32 und 64 Bit, auch Terminalserver)

- IP-Adresse:

  Die Identifikation per IP-Adresse ist nur für ein Unternehmen insgesamt möglich. Einzelne Benutzer können mit diesem Verfahren nicht unterschieden werden. Benutzer, die über die IP-Adresse identifiziert werden, surfen mit den Einstellungen des Default-Profils.

  Die Identifikation per IP-Adresse wird auch für Systeme genutzt, die ohne Benutzereingriff über den Webfilter auf Webserver zugreifen sollen, z. B. zum automatischen Download von Software-Updates.

- NTLM

  NTLM Authentisierung wird nur in lokalen Netzen in Verbindung mit einer Hornetsecurity Managed Appliance unterstützt. Über NTLM werden Benutzer gegenüber dem Webfilter automatisch mit ihrem Benutzernamen in der Windows-Domain identifiziert.

Die Authentisierung über den Hornetsecurity Connector ist die von Hornetsecurity empfohlene Variante.

2.9 LDAP-Anbindung

Der Hornetsecurity Webfilter kann über den LDAP-Dienst an das Active Directory als auch an Novells E-Directory angebunden werden. Über die Anbindung können die Nutzer mit Account-Namen, Kennwort und Gruppenzugehörigkeit synchronisiert werden. Unterstützt wird auch die Synchronisierung ausgewählter Gruppen.

Zum Schutz der Verbindung kann Secure LDAP (LDAP over SSL) oder eingesetzt oder die Verbindung über VPN getunnelt werden.

2.10 Anwendungskontrolle

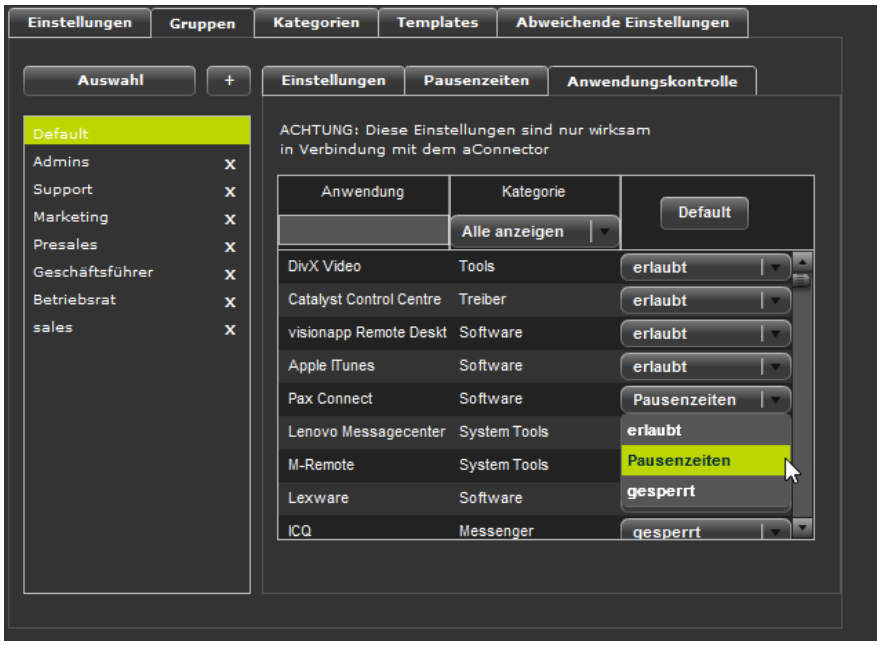

Abbildung 8: Anwendungskontrolle

Mit der Anwendungskontrolle kann der Internet-Zugriff für bestimmte Anwendungen wie z.B. Messenger (Skype, MSN, ICQ,...) komplett gesperrt, freigeschaltet oder in den Pausenzeiten für Benutzer verfügbar gemacht werden (Abbildung 8). Die Liste unterstützter Anwendungen ist erweiterbar.

Die Nutzung der Anwendungskontrolle setzt den Einsatz des Hornetsecurity Connectors auf den überwachten Clients voraus.

2.11 FTP-Transfers

Der Hornetsecurity Webfilter kann auch als FTP-Proxy eingesetzt werden. Er unterstützt FTP over SSL (FTPS) sowie FTP über SSH (SFTP). Authentisierung wird unterstützt.

2.12 HTTPS

HTTPS-Verbindungen werden vom Hornetsecurity Webfilter zunächst wie HTTP-Verbindungen über die aufgerufenen URLs überwacht und entsprechend der eingestellten Richtlinien freigegeben oder gesperrt. HTTPS-Verbindungen sind verschlüsselt, deshalb kann der Webfilter im Normalfall die in der HTTPS-Verbindung übertragenen Daten nicht analysieren und überwachen (Variante a: in Abbildung 9).

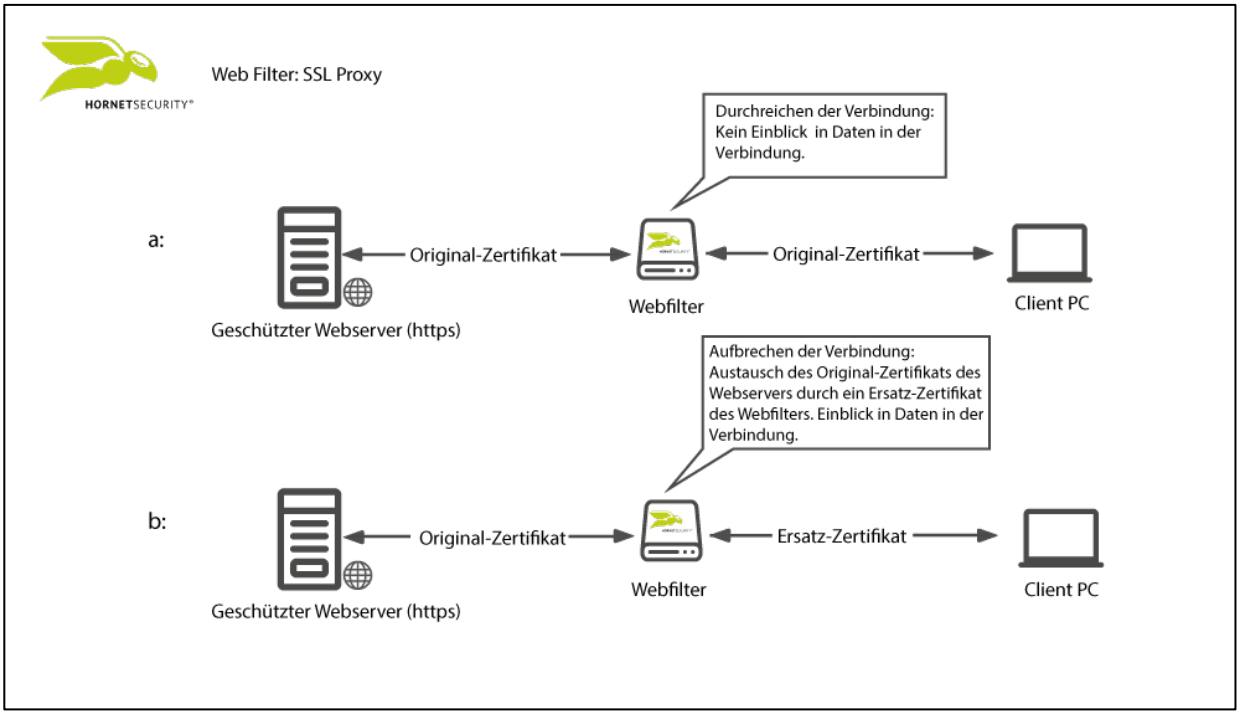

Abbildung 9: Behandlung geschützter (HTTPS) Verbindungen

Optional wird jedoch vom Webfilter das Aufbrechen von HTTPS-Verbindungen unterstützt. Verschlüsselt werden dann jeweils die Verbindung vom aufgerufenen Webserver zum Webfilter und die Verbindung vom Webfilter zum Webbrowser (Variante b: in Abbildung 9). Im Webfilter liegen die Daten dann kurzzeitig im Klartext vor und können z. B. auf Viren geprüft werden. Damit der Webbrowser dieses Aufbrechen der verschlüsselten Verbindung nicht mit einer Fehlermeldung quittiert, muss zuvor im Browser ein Zertifikat für den Webfilter als Stammzertifikat installiert werden. Alternativ kann das Stammzertifikat im unternehmensweiten Zertifikatsspeicher abgelegt werden.

2.13 Logging der Web-Aktivitäten

Die vollständige Protokollierung von Webzugriffen ist systemseitig vorgesehen und kann kundenspezifisch aktiviert oder deaktiviert werden. Eine Aktivierung bzw. Deaktivierung ist aus Datenschutzgründen nur durch den Hornetsecurity Support oder den betreuenden Hornetsecurity Partner möglich. Bei aktiver vollständiger Protokollierung werden Nutzer-ID, Zeiten und aufgerufene URLs protokolliert.

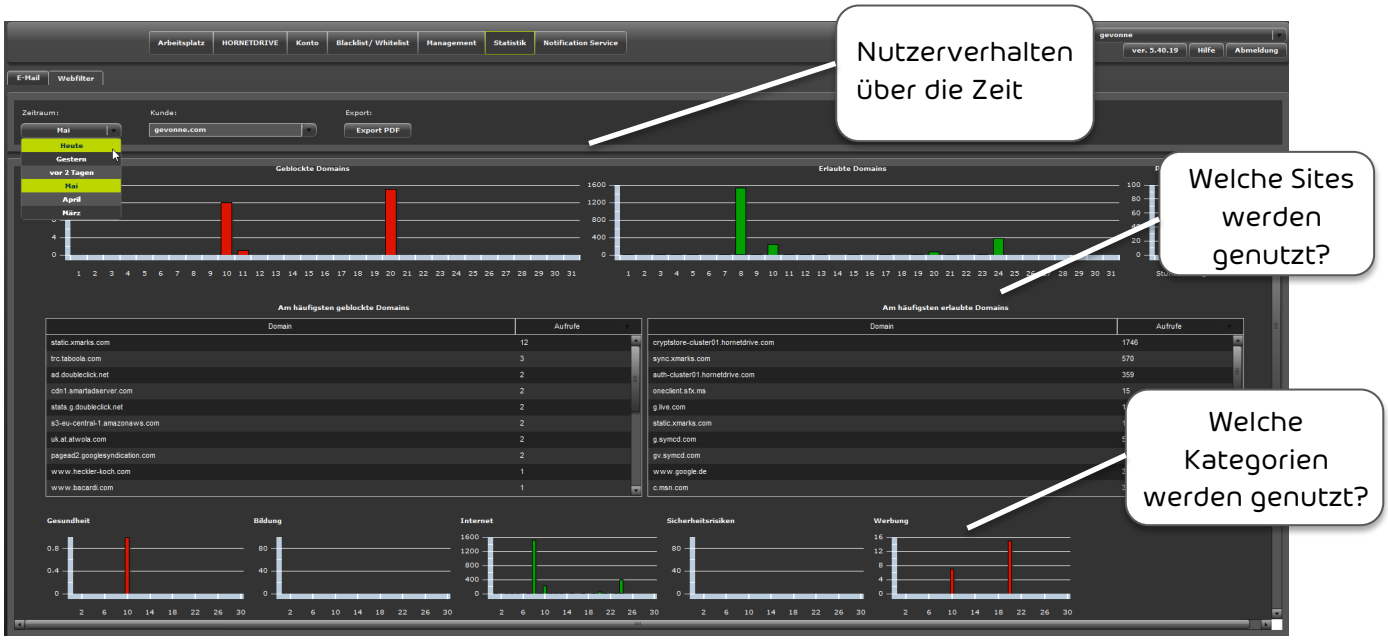

Abbildung 10: Nutzungsstatistik im Hornetsecurity Control Panel

Bei deaktivierter vollständiger Protokollierung werden die Logdaten zwar vollständig erfasst, können aber auch von Systemadministratoren nicht detailliert eingesehen werden. Eingesehen werden können nur statistische Sammeldaten (
Abbildung 10), eine Identifikation einzelner Nutzer an Hand dieser Daten ist im System nicht möglich.

Sollen bei deaktivierter vollständiger Protokollierung detaillierte Logdaten eingesehen werden, kann die vollständige Protokollierung auf Anforderung durch den Hornetsecurity Support vorübergehend aktiviert werden. Eine Einsicht in detaillierte Logdaten ist dann auch rückwirkend möglich.

2.14 Audit Log

Alle Logins von Administratoren und Benutzern sowie Konfigurationsänderungen im System werden bei Hornetsecurity automatisch protokolliert und können über das Control Panel eingesehen werden. Dadurch kann jederzeit lückenlos nachvollzogen werden, wer wann welche Konfigurationsänderungen vorgenommen hat – eine wichtige Information zur Fehlersuche im Falle von Fehlkonfigurationen (Abbildung 11).

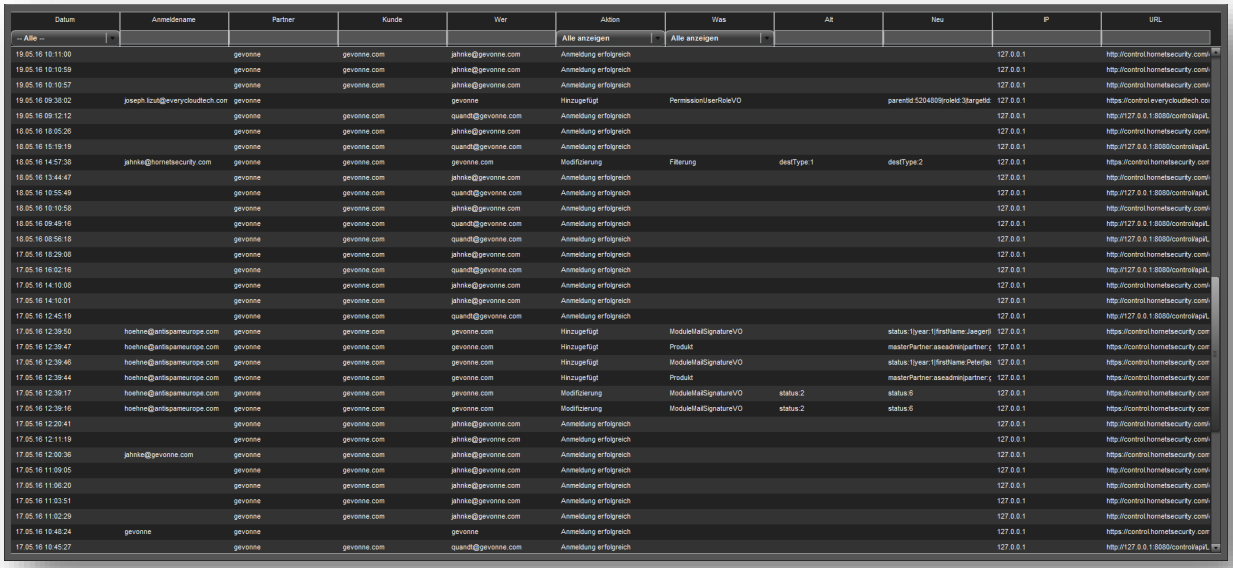

Abbildung 11: Protokollierung von Logins und Konfigurationsänderungen sind im Audit Log jederzeit nachvollziehbar

2.15 Anpassung an eigenes Corporate Design

Das Hornetsecurity Control Panel kann vollständig an das Corporate Design des Kunden oder Hornetsecurity Partners angepasst werden (Abbildung 12). Die Anpassung umfasst:

- Im Control Panel genutzte Farben
- Logo
- Templates für Spamreport (Digest) und weitere Nachrichten
- URL für das Control Panel (Optional Zugriff über Webserver des Kunden bzw. Partners, z. B. https://controlpanel.kundendomain.com/)

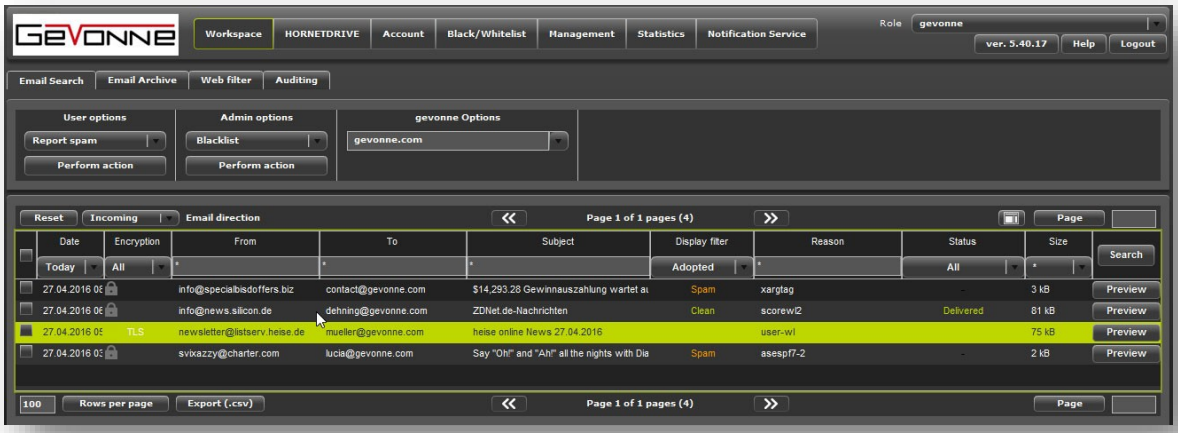

Abbildung 12: Hornetsecurity Control Panel mit Anpassung an das Corporate Design eines Kunden

2.16 Managed Appliance

Alternativ zur Nutzung des Webfilters in der Hornetsecurity Cloud kann für größere Installationen (ab ca. 500 Nutzer) auch eine antispameurope Managed Appliance zum Einsatz kommen. Mit Einsatz der Managed Appliance wird die Cloud-Lösung zur Hybrid Cloud: Der Nutzdatenverkehr läuft über die Managed Appliance im Rechenzentrum des Kunden, Steuerung und Sicherstellung des Betriebs erfolgen über die antispameurope Cloud. Zusätzlich kann der Webfilter so konfiguriert werden, dass mobile Nutzer außerhalb der lokalen Netze des Kunden über die Cloud-Variante surfen während interne Nutzer die Managed Appliance nutzen.

2.17 Leistungen im Überblick

Nachstehend sind wesentliche Eigenschaften des Hornetsecurity Webfilter Service zusammenfassend aufgeführt:

- Klassifikation von Websites nach 15 Kategorien mit bis zu 18 Unterkategorien,
- Sperre bzw. Freigabe von Websites entsprechend konfigurierbaren Unternehmensrichtlinien (Policies),
- Black- und Whitelists auf Benutzer-, Gruppen- und Systemebene,
- Freigabeanforderungen durch Benutzer möglich (konfigurierbar),
- Bearbeitung von Freigabeanforderungen durch Gruppenleiter konfigurierbar,
- Benutzerauthentifizierung per Login mit LDAP-abgleich, IP-Adresse oder über Hornetsecurity Connector,
- HTTPS-Scanning (konfigurierbar),
- Konfiguration erlaubter und verbotener Datentypen bei Downloads,
- Mehrfacher Schutz vor Schadcode,
- Automatische Proxykonfiguration über automatisch aktualisierte Konfigurationsdatei (proxy.pac),
- Detaillierte Auswertung des Webverkehrs bis auf Benutzerebene möglich (konfigurierbar),

- Umfangreiche URL-Datenbank mit über 450 Millionen Sites und 6 Milliarden Seiten in knapp 200 verschiedenen Sprachen, 100% Abdeckung der Top 1 Million Websites weltweit,
- Automatische Nachklassifikation mit manueller Qualitätssicherung bei noch nicht kategorisierten Seiten,
- Zentrales Management der Systeme durch Hornetsecurity mit 24/7/365 Überwachung und E-Mail- und Telefonsupport,
- Erhältlich als gehosteter Service mit 99,9% Verfügbarkeit aus der Hornetsecurity Cloud und als Managed Appliance im RZ des Kunden.

3 Application Programming Interface (API)

3.1 Front-End API

Alle Module des Hornetsecurity Control Panels, z. B. die Verwaltung von Freigabeanforderungen oder die Web-Statistik, können als eingebettetes Element (über das HTML-Tag „<embed>“) in eigene Web-Applikationen oder Webseiten eingebunden werden. Zur Gewährleistung des Zugriffsschutzes wird dabei ein 256-bit Authentisierungsschlüssel genutzt, der zuvor unter Angabe von Benutzername und Kennwort abgefragt werden muss. Die im Modul genutzte Sprache ist per Parameter im Aufruf einstellbar.

3.2 Back-End API

Zur engeren Einbindung in Systeme von Partnern und Kunden, aber auch zum Aufruf von Funktionen aus anderen Programmen heraus, wird von Hornetsecurity eine Back-End API bereitgestellt. Die Back-End API ermöglicht die Übermittlung von Aufrufe und Kommandos direkt an das Back-End der Hornetsecurity Cloud. Damit können z. B. Benutzer angelegt und Konfigurationen abgerufen oder verändert werden.

3.3 Voraussetzungen für die Nutzung

Voraussetzung für die Nutzung der API ist die Nutzung eines Hornetsecurity Cloud Service.
Wenn Sie die Hornetsecurity Front-End oder Back-End API nutzen wollen, nehmen Sie bitte Kontakt mit Hornetsecurity auf.

4 Webfilter Service aus Datenschutzsicht

Beim Surfen im Web werden regelmäßig personenbezogene Daten übertragen, die bei Einsatz des Hornetsecurity Webfilters auch den Webfilter passieren. Weiterhin fallen beim Surfen mit Benutzerdaten verknüpfte statistische Daten an, die ebenfalls als personenbezogene Daten im Sinne des BDSG zu

betrachten sind. Bei der Verarbeitung solcher Daten durch Hornetsecurity handelt es demnach um Datenverarbeitung im Auftrag gemäß §11, BDSG. Hornetsecurity stellt eine Vorlage für eine Datenschutzvereinbarung bereit, die Verantwortlichkeiten und Aufgaben im Rahmen der Auftragsdatenvereinbarung regelt. Bestandteil der Vereinbarung sind die von Hornetsecurity zum Schutz von Kundendaten durchgeführten allgemeinen technischen und organisatorischen Maßnahmen gemäß §9, BDSG.

Weitere, besondere Eigenschaften des Hornetsecurity Webfilter Service zum Schutz von Kundendaten:

- Nach Mandanten getrennte Datenhaltung in separaten Datenbanken,
- Zugriff auf benutzerspezifische Protokolldaten kann gesperrt werden,
- Aufbrechen von verschlüsselten Verbindungen (HTTPS) konfigurierbar und abschaltbar,
- Detailliert konfigurierbare Benutzerrechte,
- Betrieb in gesicherten Rechenzentren in Deutschland
- Mit Managed Appliance optional Betrieb im RZ des Kunden möglich

5 Quellen

- BITKOM: Jeder Zweite geht während der Arbeit privat ins Internet; http://www.bitkom.org/de/presse/70864_68878.aspx
- Wikipedia: Internetnutzung am Arbeitsplatz; http://de.wikipedia.org/wiki/Internetnutzung_am_Arbeitsplatz
- Staatsvertrag über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien (Jugendmedienschutz-Staatsvertrag - JMStV)
- WhiteHat Security: WhiteHat Website Security Statistics Report; https://www.whitehatsec.com/assets/WPstats_winter11_11th.pdf

Hornetsecurity GmbH · Am Listholze 78 · 30177 Hannover
Tel.: +49 511 515 464-0 · info@hornetsecurity.com · www.hornetsecurity.com
Umsatzsteuer-ID: DE256599255 · Geschäftsführer: Oliver Dehning, Daniel Hofmann, Daniel Blank · Amtsgericht Hannover · HRB 201937
Hannoversche Volksbank · IBAN: DE74 2519 0001 0573 5742 00 · BIC: VOHADE2H