Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IM UNTERNEHMEN

Next Generation Firewalls

Empfehlung von Einsatzmöglichkeiten für den normalen Schutzbedarf

Die sogenannten Firewalls „der nächsten Generation“ bieten neben den in großer Zahl in die Next Generation Firewalls (NGFW) integrierten Sicherheitskomponenten die Möglichkeit, Applikationsdaten[1] im Datenstrom zu erkennen. In dieser Empfehlung werden die Eigenschaften einer NGFW betrachtet und zugleich sinnvolle Einsatzmöglichkeiten unter Berücksichtigung von ISi-LANA[2] aufgezeigt.

Die Vorteile einer Next Generation Firewall sind abhängig von Funktionsumfang und insbesondere Qualität der integrierten Sicherheitskomponenten, die zentralisiert die System- und Netzwerkinformationen sammeln, verarbeiten und darstellen. Durch die in großer Zahl vorhandenen Sicherheitskomponenten wird angestrebt, organisatorische und logische Abläufe eines Unternehmens durch den Einsatz von NGFWs in konsistenter Weise zu berücksichtigen und die IT entsprechend auf Netzwerkebene zu regeln bzw. zu schützen. Mithilfe umfangreicher und dennoch übersichtlich gestalteter Regelsätze (Security-Policies) können NGFW hierzu einen Beitrag leisten.

Die Hersteller von NGFW gestalten den Funktionsumfang sowie die technische und logische Abarbeitung der Regelsätze sehr unterschiedlich. Für die konkrete Auswahl eines Produktes sollten die Eigenschaften sorgfältig gesichtet und den jeweiligen Einsatzbedingungen im IT-Betrieb gegenübergestellt sowie beurteilt werden. Grundsätzlich sind die Anforderungen an einer NGFW bzw. deren integrierten Sicherheitskomponenten nicht anders zu beurteilen als herkömmliche Sicherheitslösungen. Eine ausführliche Hilfestellung für die Beurteilung von Sicherheitslösungen, u. a. welche Anforderungen erfüllt sein sollten, können die Studie ISi-LANA oder auch die anderen Module aus der ISi-Reihe[3] bieten.

Zum Verständnis der folgenden Ausführungen sei zuvor auf die Differenzierung zwischen einem Applikation Level Gateway (ALG) und einer NGFW hingewiesen, da sich die beiden Sicherheitslösungen grundlegend unterscheiden, insofern die Art und Weise der Kommunikationsverbindung von Client zum Server (Ende-zu-Ende-Verbindung) betrachtet wird.

Ein ALG muss immer eine neue Netzwerkverbindung zum Zielsystem initialisieren, damit keine direkte Verbindung vom Client zum Zielsystem besteht. Damit übernimmt ein ALG die Rolle des Stellvertreters (Proxy) für den Client. Durch vorhandene Filterfunktionen oberhalb der Transportschicht kann die Einhaltung von Netzwerk- und Anwendungsprotokollen erzwungen werden. Zusätzlich zu den Filterfunktionen auf Da-

1 Identifizieren von Anwendungen und Anwendungsprotokollen, unabhängig von Port-Nummern.
2 Sichere Anbindung von lokalen Netzen an das Internet (Isi-LANA): https://www.bsi.bund.de/dok/6620614
3 BSI-Standards zur Internet-Sicherheit (Isi-Reihe): https://www.bsi.bund.de/ISi-Reihe

teninhalte besteht oft die Möglichkeit, bestimmte Inhalte bei Bedarf zu verändern. Der Funktionsumfang und die Sicherheitsaspekte bzw. deren Umsetzung sind abhängig vom Herstellerprodukt.

Eine NGFW verarbeitet die Netzwerkpakete selektiv und leitet diese im Gegensatz zu ALGs durch ein Routing (bzw. Forwarding) oder Bridging weiter, sofern die Netzwerkpakete der Freigabekonformität der NGFW (u. a. der Regelsätze) entsprechen. Häufig werden weitere Analyseschnittstellen zur Verfügung gestellt, z. B. durch integrierte Netzwerk TAPs[4]. Die Netzwerk- und Anwendungsprotokolle oberhalb der Transportschicht werden bei einer NGFW anhand von Signaturen bzw. Mustern nach bestimmten Auffälligkeiten überprüft und können dementsprechend in den Regelsätzen berücksichtigt werden. Dateninhalte können (wenn überhaupt) meist nur sehr begrenzt verändert werden. Eine NGFW enthält jedoch auch integrierte Proxies, z. B. einen erforderlichen Secure Sockets Layer (SSL/TLS)-Proxy.

Sowohl bei ALG als auch NGFW kommen zur Unterstützung ggf. heuristische Verfahren zum Einsatz. Zum Beispiel können diese bei einem ALG zum Herausfiltern von Java-Script-Code innerhalb einer HTML[5]-Seite oder bei einer NGFW für die Identifizierung von Applikationen genutzt werden.

Sind die Eigenschaften eines ALGs erforderlich, so kann dieses prinzipiell nicht durch eine NGFW ersetzt werden. Dies ist z. B. dann der Fall, wenn für den Aufbau einer P-A-P[6]- Struktur nach ISi-LANA die strikte Netztrennung oder die umfassende Proxy-Fähigkeit des ALGs erforderlich ist. Allerdings kann es je nach Anforderungen sinnvoll sein, eine NGFW als höherwertigen Paketfilter in dieser Struktur zu betreiben.

1 Die Sicherheitskomponenten einer NGFW

Die integrierten Sicherheitskomponenten können einen bedeutenden Beitrag zum Sicherheitsniveau der IT-Infrastruktur bieten. Zusätzlich zur Produktauswahl müssen auf jeden Fall die Ressourcen für die Administration einkalkuliert werden.

Eine NGFW sollte die grundlegenden Kommunikationsverbindungen (wer kommuniziert wie mit wem zu welchem Zeitpunkt) detailliert kontrollieren können, geeignete Schutzmaßnahmen anbieten und gute Protokollierungs- sowie Berichtsfunktionen mitbringen. Die Protokollierung sowie die Analyse von Kommunikationsbeziehungen muss konfigurierbar und deaktivierbar sein.

Wenn eine NGFW aufgrund ihrer Eigenschaften als ein höherwertiger Paketfilter eingesetzt wird, sollten diese und ebenfalls alle weiteren Anforderungen nach ISi-LANA erfüllt sein.

Folgende Sicherheitskomponenten sollten unterstützt werden:

- ✔ Herkömmliche Funktionen einer Stateful Inspection Netzwerk-Firewall (Paketfilter) einschließlich eines Bandbreitenmanagements (Quality of Service).
- ✔ Anwendungsidentifizierung und -filterung: Identifizieren und Filtern von Anwendungen und Anwendungsprotokollen, unabhängig von Port-Nummern.
- ✔ Ein integrierter Schutz vor Malware für die Überprüfung des Netzwerkverkehrs.
- ✔ Die Möglichkeit der Entschlüsselung von Secure Sockets Layer (SSL)-Verbindungen bzw. Transport Layer Security (TLS)-Verbindungen durch einen SSL/TLS-Proxy. Dafür müssen eine Zertifikatsverwaltung sowie Überprüfungsmechanismen der Zertifikate auf ihre Gültigkeit vorhanden sein. Der SSL/TLS-Proxy sollte möglichst allgemein für SSL/TLS-Verbindungen genutzt werden können, z. B. nicht nur für Browser-Anwendungen. Außerdem sollte eine Entschlüsselung von SSH-Verbindungen durch einen SSH-Proxy möglich sein.

4 Test Access Ports (TAPs) können die Daten auf der Leitung analysieren, ohne den Netzwerkverkehr aktiv zu beeinflussen.
5 Hypertext Markup Language (HTML)
6 P-A-P (Paketfilter - Applikation Level Gateway - Paketfilter)

- ✔ Ein integriertes Network Intrusion Detection System (NIDS) und Network Intrusion Prevention System (NIPS).
- ✔ Eine Benutzerauthentifizierung und -identifizierung für benutzerspezifische Regelsätze. Neben einer lokalen Benutzerauthentifizierung sollten sich externe Quellen, wie Verzeichnisdienste (z. B. LDAP-fähige) oder Benutzerauthentifizierungsdienste (z. B. Radius-Server), einbinden lassen.
- ✔ Das Blockieren von Dateien aus dem Netzwerkverkehr, z. B. von ausführbaren Dateien.
- ✔ Ein integrierter URL-Filter mit Black- und Whitelisting - Verfahren. Es sollten kategorisierte Listen unterstützt werden, die bei Bedarf regelmäßig vom Hersteller aktualisiert und vom Administrator individuell erweitert werden können, z. B. durch zusätzliche Listen.
- ✔ (Bei Bedarf): Ein integriertes Data Leakage Prevention (DLP) System oder integrierte DLP-Funktionalitäten.
- ✔ (Bei Bedarf): Eine integrierte Virtual Private Network (VPN) - Gegenstelle, um einen sicheren Fernzugriff auf die lokalen Netze anbieten und/oder Standorte sicher miteinander verbinden zu können.
- ✔ (Optional): Spamfilter
- ✔ (Optional): Integrierte Proxies (z. B. für World Wide Web - Dienste). Proxies sollten innerhalb einer gesicherten Umgebung (z. B. mithilfe von Sandbox-Techniken) des Betriebssystems ausgeführt werden, insbesondere da Proxies als Stellvertreter der Clients fungieren und somit auch direkt von möglichen Schwachstellen bedroht werden können.
- ✔ (Optional): Ein integriertes Network Access Control (NAC).

Folgende Eigenschaften sollten unterstützt werden:

- ✔ Die Sicherheitskomponenten sollten übersichtlich dargestellt werden können, z. B. einstufig in einem Regelsatz. Ein Regelsatz kann z. B. bestehen aus Paketfilter-, Anwendungs- und Protokoll-Regeln sowie Malware-Erkennung, NIPS, Benutzerrollen, etc.
- ✔ Automatische kalender-, wochentag- sowie tageszeitabhängige Aktivierung bzw. Deaktivierung der Regelsätze.
- ✔ Konfigurationsänderungen müssen ohne Unterbrechung des Netzwerkverkehrs möglich sein.
- ✔ Konfigurierbares Rechtekonzept des Systems, damit organisatorische Administrationsrollen dargestellt werden können.
- ✔ Eine zentrale Verwaltung (Management) des kompletten Systems. Ein Out-of-Band-Management sollte vorhanden sein.
- ✔ Ausführliche (aufbereitete) Berichts- und Analysefunktionen zur Darstellung der gesamten Netzwerkaktivitäten.
- ✔ Die Protokollierungs- und Berichtsfunktionen sollten zielgerichtet und detailliert (z. B. über die Regelsätze) zu gestalten sein. Eine Protokollierung sowie die Aufnahme von Netzwerkverkehr in die Berichtsfunktionen darf nicht zwingend sein.
- ✔ Eine regelmäßige Aktualisierung aller Signaturdatenbanken, die manuell/automatisch online möglich sein sollten. Bei Bedarf sollten auch offline-Aktualisierungen möglich sein.
- ✔ Signaturupdates sollten vor der Aktivierung nachvollziehbar dokumentiert sein. Die NGFW sollte die Möglichkeit anbieten, wieder auf den vorherigen Signaturstand zurückzukehren.
- ✔ Sofern eine Verbindung ausgehend der NGFW zum Hersteller erwünscht ist, z. B. für eine Online-Aktualisierung oder für eine Anbindung in der Cloud des Herstellers, sollte diese Verbindung analog zu den Administrationsschnittstellen ausreichend verschlüsselt werden.
- ✔ Damit das System zuverlässig für die erforderlichen Einsatzzwecke ausgewählt und administriert werden kann, ist es sehr wichtig, die Funktionsweise der einzelnen Sicherheitskomponenten zu verstehen. Als Hilfestellung sollten die Hersteller Ablaufpläne (z. B. mithilfe von Datenflussdiagrammen) anbieten, die die konkrete Abarbeitung der Regelsätze erläutert. Dadurch sollte auch ersichtlich werden, welche Kriterien zu welchen Aktionen führen. Der Gültigkeitsbereich von Anwendungsfreigaben sollte daraus ebenfalls hervorgehen.
- ✔ Alle Sicherheitskomponenten sollten bereits möglichst umfassend die Funktionen des IPv6-Protokolls abdecken und sofern vorhanden, unbedingt beherrschen. Für noch ausstehende IPv6-Umsetzungen der NGFW sollte der Hersteller einen Zeitplan bereitstellen können. Anmerkung: Besonders in den ersten Jahren der IPv6-Einführung besteht die große Herausforderung, alle Funktionen des komplexen IPv6-Protokolls abzudecken und fehlerfrei zu beherrschen.

- ✔ (Optional): Die Überprüfung von Netzwerkverkehr in der Cloud des Herstellers ist optional. Ist die Funktion vorhanden, muss diese deaktivierbar sowie konfigurierbar sein. Um möglichst viele Einsatzmöglichkeiten berücksichtigen zu können, sollte konfigurierbar sein, ob und wenn ja, in welcher Form Dateien in der Cloud übertragen werden dürfen (z. B. nur Hashwerte einer Datei oder die komplette Datei).
- ✔ [Wäre bei Bedarf wünschenswert]: Die Möglichkeit, Netzwerkverbindungen einem Benutzer zuzuordnen, ohne die IP-Adresse des Benutzers heranzuziehen zu müssen. Dieses kann z. B. für den Einsatz eines Terminalservers erforderlich werden, falls dieser dem Benutzer keine eigene IP-Adresse zuweist. Die Zuordnung von Netzwerkverbindungen zu einem Benutzer könnte mithilfe eines Agenten auf dem System (z. B. auf einem Terminalserver) erfolgen.

2 Anwendungsidentifizierung und -filterung

Ein besonderer Mehrwert einer NGFW kann die Anwendungsidentifizierung und -filterung sein. Aus diesem Grund wird im Folgenden gesondert darauf eingegangen.

Im Datenstrom wird nach signifikanten und/oder nach charakteristischen Auffälligkeiten gesucht. Wird eine Anwendung (z. B. aus dem Bereich Peer-to-Peer) oder Funktionen einer Anwendung (z. B. eingebettete Chat-Funktion) identifiziert, sollte die Möglichkeit bestehen, diese zu protokollieren, oder zu blockieren, ggf. Alarm auszulösen oder – falls diese Anwendungen der Regelkonformität des Unternehmens nicht widersprechen – sie auch freizugeben. Die Anwendungsfilterung sollte es ermöglichen, dass nicht identifizierter Netzwerkverkehr grundsätzlich blockiert wird. Bei Bedarf sollte es jedoch auch möglich sein, nicht identifizierten Netzwerkverkehr freizugeben, z. B. für Netzwerkverkehr, der für eine Anwendung erforderlich ist, jedoch noch nicht von der Anwendungsidentifizierung berücksichtigt wird. In diesem Fall müssen weitere Analysemöglichkeiten für diesen Netzwerkverkehr bestehen, um diesen bei Bedarf gezielt zu beobachten und analysieren zu können. Aus den daraus gewonnen Informationen könnten je nach Szenario z. B. individuelle Anwendungssignaturen bzw. -muster erstellt werden oder der Netzwerkverkehr gezielt auf IP-Netzwerkebene eingeschränkt werden.

Folgende Eigenschaften sollten unterstützt werden:

- ✔ Die NGFW sollte so justierbar sein, dass nur freigegebene Anwendungen die NGFW passieren dürfen. Dieses setzt eindeutige zielgerichtete Definitionen der Anwendungen voraus, die dementsprechend von der Anwendungsidentifizierung berücksichtigt und eingehalten werden müssen.
- ✔ Eine umfangreiche Berücksichtigung gängiger und proprietärer Anwendungen ist notwendig, damit der Netzwerkverkehr priorisiert nach Anwendungen geregelt werden kann. Neue, bisher von der NGFW noch nicht berücksichtigte Anwendungen, sollten mithilfe individueller Signaturen bzw. -muster erfasst werden können.
- ✔ Nicht erkannter Anwendungsdatenverkehr sollte in der Protokollierung entsprechend gekennzeichnet und in einer Übersicht (z. B. Gefährdungslage) dargestellt werden können.
- ✔ Insbesondere nicht identifizierter Anwendungsdatenverkehr sollte bei Bedarf (konfigurierbar) automatisch weitere Analysemechanismen durchlaufen können, z. B. eine Analyse auf Anzeichen von Netzwerkangriffen. Dieses kann auch mithilfe integrierter Sicherheitskomponenten (z. B. IDS/IPS) realisiert werden.
- ✔ Netzwerkverkehr sollte bei Bedarf (konfigurierbar) gezielt aufgezeichnet und in gängigen Formaten (z. B. PCAP) gespeichert werden können, um z. B. nicht identifizierten Anwendungsdatenverkehr analysieren zu können.
- ✔ Eine Dokumentation der berücksichtigten Anwendungen, die eindeutig die Einsatzbedingung und Funktion der Anwendung beschreibt, sollten existieren.
- ✔ Zur Erweiterung der Anwendungsidentifizierung sollten individuelle Signaturen bzw. Muster erstellt werden können, die auf grundlegende Netzwerkprotokolle angewendet werden können, z. B. auf IP-, UDP-, TCP-Protokolle.
- ✔ Für die Erstellung individueller Signaturen bzw. Muster sollten auch gezielte Eingabemasken zur Verfügung stehen, die standardisierte Protokollparameter (z. B. Hypertext Transfer Protocol -Parameter) berücksichtigen.
- ✔ Die Signatur- bzw. Mustererstellung sollte reguläre Ausdrücke berücksichtigen. Die erstellten Signaturen- bzw. Muster sollten kombinierbar sein.

3 Mögliche Problemstellungen beim Einsatz einer NGFW

Besteht eine Netzwerkverbindung (z. B. für Signaturupdates, eine Anbindung an die Cloud, etc.) über das Internet vom NGFW-System zum Herstellerportal, so kann dieser Netzwerkverkehr aufgrund der notwendigen Verschlüsselung nicht kontrolliert werden. Hier besteht die Gefahr, dass vertrauliche Daten an Dritte preisgegeben werden. Aber auch unabhängig von der Verschlüsselung können Fehlkonfigurationen durch den Administrator, z. B. in der Festlegung welcher Netzwerkverkehr in der Cloud überprüft werden darf, unter Umständen dazu führen, dass ungewollt vertrauliche Informationen in der Cloud versendet werden könnten.

Besonders Anwendungen von hoher Verfügbarkeit lassen sich unter Umständen aus organisatorischen Gründen nicht oder nur bedingt von der Anwendungsfilterung berücksichtigen, da ein falsches Erkennungsergebnis der Anwendungsidentifizierung gravierende Folgen haben könnte.

Vor der Nutzung der NGFW sollen die rechtlichen Aspekte berücksichtigt worden sein, insbesondere wenn die private Nutzung betrieblicher Kommunikationsmittel erlaubt ist. Aus Sicherheitssicht wird die Speicherung der Protokolldaten für eine Speicherdauer von drei Monaten für sinnvoll gehalten, z. B. für Zwecke der Forensik.

Wesentliche Sicherheitsfunktionen basieren auf den vom Hersteller zur Verfügung gestellten Signaturen. Daher ist darauf zu achten diese aus vertrauenswürdigen Quellen regelmäßig zu aktualisieren.

Eine besondere Herausforderung an die NGFW besteht darin, bei komplexeren Regelsätzen einen guten Netzwerkdatendurchsatz zu gewährleisten. Der erforderliche Netzwerkdatendurchsatz sollte bei der Auswahl des Produktes angemessen berücksichtigt sowie Leistungsreserven eingeplant werden. Die benötigten Netzwerkdurchsatzraten und die benötigte Komplexität der Regelsätze sollten mit dem Hersteller oder ggf. einem IT-Dienstleister besprochen und von diesem vertraglich zugesichert werden können. Kann dies nicht garantiert werden, müssen zusätzliche Sicherheitslösungen implementiert werden, die diese Anforderungen erfüllen.

Sollten sich die benötigten Bedingungen des Unternehmens nicht insgesamt durch die integrierten Funktionen einer NGFW abbilden lassen, müssen diese durch weitere Maßnahmen (z. B. basierend auf ISi-LANA oder den anderen Modulen der ISi-Reihe) geschaffen werden.

Unter Umständen kann der große Funktionsumfang dazu führen, dass die NGFW ein höheres Angriffspotenzial bietet, falls sich die integrierten Sicherheitskomponenten nicht optimal an die Einsatzbedingungen anpassen lassen oder nicht benötigte Funktionen keine Deaktivierungsmöglichkeiten besitzen. Dies könnten z. B. Schwachstellen, unsichere Zugänge oder Erschöpfung von Leistungsreserven (Bandbreite, physische Systemressourcen u.a. CPU sowie Controller) sein.

Offene bzw. herstellerunabhängige Programmier-Schnittstellen (API[7]) werden derzeit kaum angeboten.

7 Application Programming Interface (API)

4 Einsatzmöglichkeiten für den normalen Schutzbedarf

4.1 Für kleine Unternehmen mit wenigen Clients

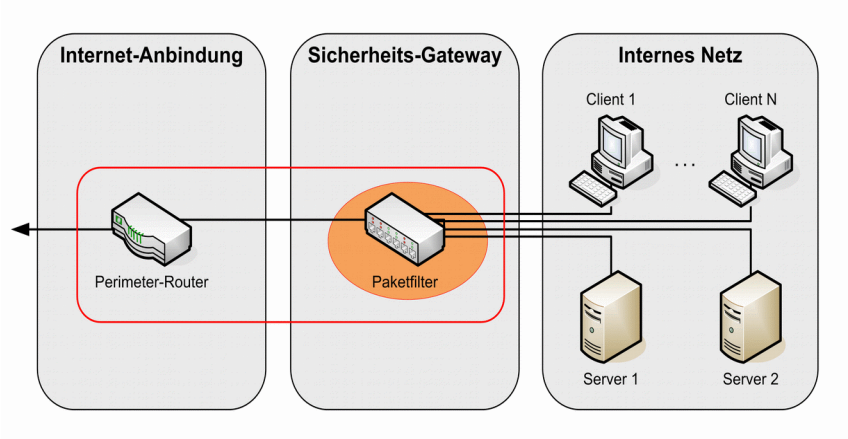

Abbildung 1: Normaler Schutzbedarf für kleinere Unternehmen (Quelle ISi-LANA)

Eine NGFW könnte in diesem Fall an der Position des Paketfilters (PF) bereits wesentliche Schutzfunktionen bereitstellen. Die meisten NGFW können bereits mit wenig Konfigurationsaufwand einen sehr guten Basisschutz für kleinere Unternehmen mit angemessenem Aufwand und Kosten darstellen. Viele Hersteller bieten für kleinere Unternehmen Komplettsysteme an, die im Funktionsumfang kaum weniger bieten als die höher performanten Firewall-Komplettsysteme im gleichen Herstellersortiment.

Der Perimeter-Router und der Paketfilter (PF) können entsprechend ISi-LANA unter bestimmten Einsatzbedingungen zusammengelegt werden.

4.2 Für große Unternehmen mit ausgeprägter Netzinfrastruktur

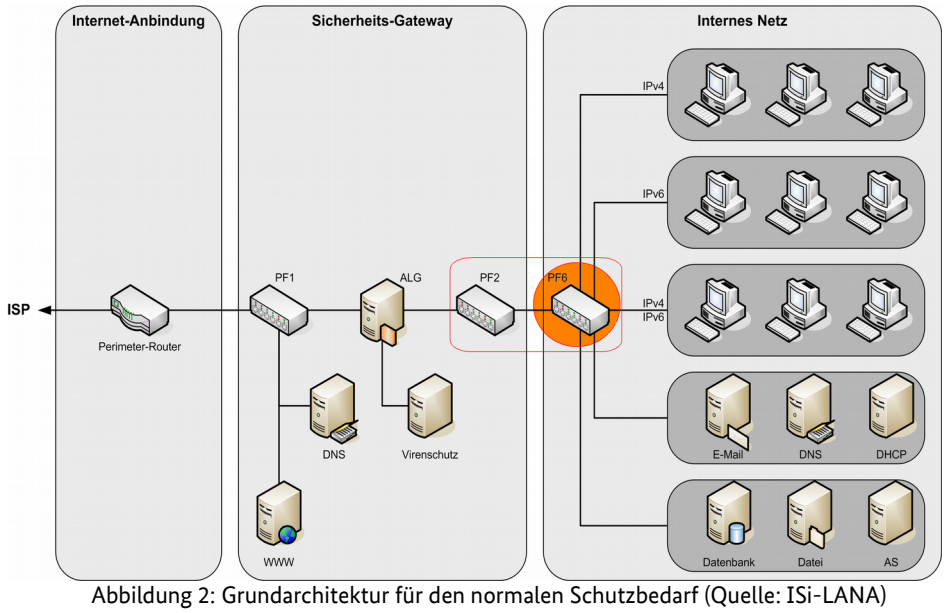

Abbildung 2: Grundarchitektur für den normalen Schutzbedarf (Quelle: ISi-LANA)

Der Einsatz einer NGFW könnte in diesem Fall an der Position des Paketfilters (PF6) eine gute Ergänzung zur bestehenden Netzinfrastruktur sein. An dieser Position kann eine NGFW frühzeitig ihre Vorteile durch die integrierten Sicherheitskomponenten einbringen.

Das ALG könnte in Richtung des Internets die primäre Aufgabe der Protokoll-Verifizierung (z. B. für HTTP, SMTP) übernehmen und als Stellvertreter des Clients (keine direkte Internetverbindung) fungieren sowie die Möglichkeit bieten, Dateninhalte verändern zu können. Die NGFW könnte mithilfe der Anwendungsidentifizierung den Netzdatenverkehr zielgerichtet regeln bzw. erfassen und damit das ALG ergänzen und entlasten. Durch die zentrale Position des Paketfilters (PF6) ist die NGFW in der Lage, das komplette Datenaufkommen zwischen den Netzwerkbereichen im Intranet zu erfassen und zu verarbeiten.

Die Paketfilter (PF2) und (PF6) können entsprechend ISi-LANA unter bestimmten Einsatzbedingungen zusammengelegt werden.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **info@cyber-allianz.de** gesendet werden.