genua

Datendiode vs-diode

Hochperformante und zuverlässige
One Way-Schnittstellenlösung für Schwarz-Rot-Übergänge

Technische Informationen

genua

Inhaltsverzeichnis

1 Das Wichtigste zuerst und in Kürze

Die vs-diode für den Geheimschutzbereich ist eine Weiterentwicklung der bewährten genugate-Datendiode von genua. Das Hochsicherheitssystem transferiert Daten nur in eine Richtung von schwarzen in rote Netze und ist damit komfortabler und schneller als ein sogenanntes Air-Gap, also ein manueller Transfer mit Speichermedien in höher eingestufte Netze.

Aufgrund ihrer gesicherten Datenübertragung mit Empfangsbestätigung ist die vs-diode verlässlicher als eine Glasfaserdiode. Die Trennung der Komponenten erfolgt mit physisch getrennter Hardware sowie Separation durch einen L4-Microkernel. Damit reicht die Sicherheit des Systems über die einer Firewall hinaus. Die vs-diode basiert auf der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach CC EAL 4+ zertifizierten und zusätzlich als „Highly-Resistant“ eingestuften Firewall genugate. Sie ist vom Bundesamt für Sicherheit in der Informationstechnik bis zur VS-Stufe GEHEIM zugelassen.

In dieser Informationsbroschüre stellen wir die Lösung, Funktionen und Einsatzbereiche vor.

2 vs-diode: Zuverlässiger Einbahndatentransfer an Schwarz-Rot-Übergängen

Diese Broschüre richtet sich an Personen und Einrichtungen, die mit vertraulichen und nach VS-Anweisung eingestuften Informationen arbeiten und Vorkehrungen zu deren Schutz zu treffen haben.

Sie bietet Ihnen einen kompakten Überblick, wie Sie mit Hilfe der vs-diode den kontrollierten, sicheren Einbahndatentransfer von schwarzen, unklassifizierten in rote, klassifizierte Netze ermöglichen.

2.1 Problemstellung

Die meisten Netzwerke benötigen Zugang zu aktuellen Daten, die sie aus anderen Netzen beziehen. In aller Regel wirft der Datenaustausch keine Probleme auf – bei Netzen in unterschiedlich eingestuften Bereichen ist dagegen eine direkte physikalische Kopplung aus Sicherheitsgründen nicht akzeptabel.

Der Datentransfer zu einem höher eingestuften Bereich erfolgt in diesen Fällen vielfach manuell, d. h. durch den Einsatz von portablen Speichermedien wie CD-ROMs oder USB-Sticks. Die zu übertragende Information wird also zunächst von der niedriger eingestuften Datenquelle auf das portable Medium übertragen, von dem die Information anschließend in das höher eingestufte Netz eingespielt wird. Ein Datentransfer in umgekehrter Richtung lässt sich durch entsprechende Instruktionen des zuständigen Personals vermeiden.

Problematisch an dieser Methode ist, dass kein Echtzeittransfer erfolgen kann und der Einsatz portabler Datenträger im Umgang mit vertraulichen Informationen ein ernsthaftes Sicherheitsrisiko birgt.


Eine bessere Lösung stellen automatisierte bzw. teilautomatisierte Hochsicherheits-Gateways zur kontinuierlichen Kopplung unterschiedlich eingestufter Netze dar, die wir im nächsten Abschnitt beschreiben.

2.2 Lösungen – Typen von Hochsicherheits-Gateways

Unterschiedliche Lösungsansätze verfolgen Paketdioden, Datendioden und Rot-Schwarz-Gateways.

2.2.1 Paketdioden

Paketdioden können nur einzelne IP-Pakete in ausschließlich einer Richtung – von Schwarz nach Rot – transferieren, während die Rückrichtung gänzlich unterbunden ist. Ein Abfluss eingestufter Informationen kann somit ausgeschlossen werden. Umgesetzt wird dies durch eine Glasfaserverbindung, bei der die Faser für die Rückrichtung nicht angeschlossen ist. Auf dieser Verbindung kann nur das User Datagram Protocol (UDP) gesprochen werden.

Dieses Protokoll bringt den Nachteil mit sich, dass es selbst bei mehrfacher Übertragung keine Garantie für den Empfang eines einmal gesendeten Pakets gibt. Daten können demnach unvollständig empfangen werden und damit unbrauchbar sein. Per UDP übermittelte Pakete müssen ferner nicht in der gesendeten Reihenfolge ankommen oder können mehrfach beim Empfänger eintreffen. Deshalb müssen Anwendungen, die UDP nutzen, gegenüber verloren gegangenen und unsortierten Paketen unempfindlich sein oder entsprechende Korrekturmaßnahmen mitbringen. Transfers größerer zusammenhängender Datenmengen sind fast unmöglich, da keine Bestätigung über den Empfang der einzelne Pakete zurück übermittelt werden kann und der Absender daher nie genau weiß, ob die Daten vollständig angekommen sind.

2.2.2 Datendioden

Datendioden ermöglichen die Datenübertragung von Schwarz nach Rot, basierend auf dem Transmission Control Protocol (TCP), das jedoch einen gleichzeitigen Paketaustausch in beide Richtungen erfordert. Dabei gewährleisten – im Gegensatz zur Paketdiode – die Kontrollpakete von TCP einen sicheren, kontrollierten Datentransfer. Übertragungsfehler, verlorene Datenpakete oder Duplikate werden vermieden.

Allerdings muss am Übergang sichergestellt werden, dass jegliche Rückpakete bis auf die für den Kommunikationsprozess essentiell notwendigen Protokoll-Daten normalisiert werden – also keine versteckten Informationen enthalten. Neben die Anforderung der maximalen Datensicherheit tritt bei diesem Lösungsansatz das Ziel der maximalen Übertragungssicherheit. Die Erfüllung dieser Anforderungen stellt das Key Feature einer Datendiode dar.

2.2.3 Rot-Schwarz-Gateways

Ein Rot-Schwarz-Gateway ermöglicht die exakte inhaltliche Kontrolle und Steuerung des Datenflusses zwischen unterschiedlich eingestuften Netzen – von Schwarz nach Rot und von Rot nach Schwarz. Dies kann mit Hilfe verschiedener Sicherheitskomponenten realisiert werden. Eine Möglichkeit stellt z. B. ein zweistufiges Verfahren mittels Prüfserver und

Sicherheitsfilter dar. Die Inhaltskontrolle kann dabei sowohl automatisiert als auch manuell erfolgen.

Bei maschinellen Verfahren prüft ein Parser die Dateien, deren Inhalt in ein genau definiertes Format eingebettet ist. Dagegen sind Dateien mit beliebigen Texten oder Grafiken vom Anwender manuell mit einem Viewer zu prüfen. Im Gegensatz zur Paket- und Datendiode hat dieser Lösungsansatz also auch die Funktion, exakt definierte Informationen, die von ihrer Natur her schwarz sind, von Rot nach Schwarz zu transferieren.

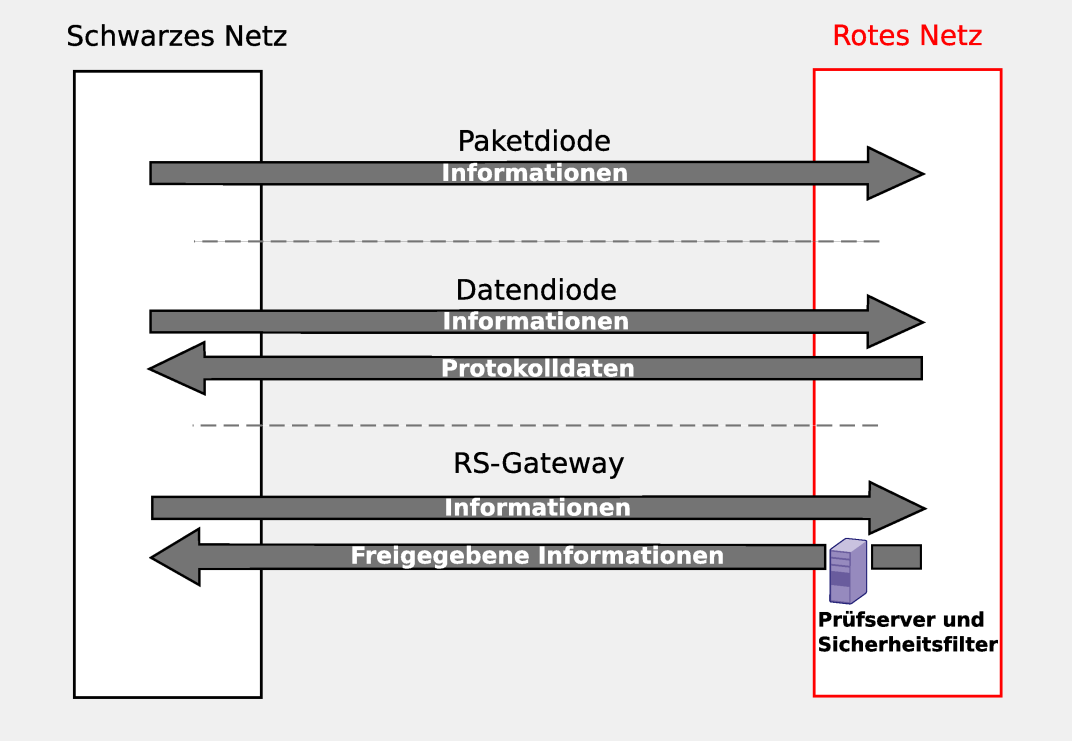

Abb. 1: Schematische Übersicht: Abgrenzung Paketdiode, Datendiode und Rot-Schwarz-Gateway

Zur restriktiven Kontrolle kritischer Übergänge können wir Ihnen je nach Anforderungsprofil Paket- und Datendioden sowie Rot-Schwarz-Gateways anbieten.

3 Sicherung von Verschlusssachen

3.1 Verschlusssachenanweisung und Schwarz-Rot-Kopplung

Die Vertraulichkeit, Verfügbarkeit und Integrität von Daten ist mit Schutzmaßnahmen entsprechend dem Stand der Technik zu gewährleisten, fordert sinngemäß die VS-Anweisung vom Bundesministerium des Innern. Dementsprechend muss die Möglichkeit einer Kopplung unterschiedlicher Sicherheitsdomänen in betroffenen Organisationen unter Sicherheitsaspekten umfassend geprüft werden. An Übergängen sind geeignete Vorkehrungen zu treffen.


3.2 Geheimschutz stellt besondere Systemanforderungen

An eine Schnittstellenlösung zwischen unterschiedlich eingestuften Netzen werden demnach besondere Anforderungen gestellt: Sie muss einerseits eine Übertragung schädlicher Programme vom schwarzen ins rote Netz verhindern und andererseits zuverlässig gewährleisten, dass keine Daten aus einem höher eingestuften Bereich in einen niedriger eingestuften gelangen.

Soll die Schnittstellen-Lösung zusätzlich eine kontrollierte Datenübermittlung in ein rotes Netz ermöglichen, ist – wie bereits angesprochen – ein Rückfluss von Statusinformationen erforderlich. Eine bidirektionale Kommunikation stellt in diesem Umfeld jedoch ein Sicherheitsrisiko dar, dem mit einer geeigneten Systemarchitektur zu begegnen ist.

4 Die Anforderungen im Einzelnen

Im Folgenden gehen wir auf die grundsätzlichen Anforderungen ein, die eine Datendiode an Schwarz-Rot-Übergängen erfüllen muss.

4.1 Funktionelle Anforderungen

4.1.1 Datentransfer von Schwarz nach Rot

Datenkommunikation zwischen zwei Endgeräten in verschiedenen Netzen setzt zunächst ein IP-basiertes System voraus, das sichere Übertragungsverfahren bereitstellt.

4.1.2 Verlässlichkeit

Ein Datenverlust ist durch ein entsprechendes Übertragungsprotokoll auszuschließen. Den Erfolg bzw. Misserfolg des Transfers soll eine Statussignalisierung dokumentieren.

4.1.3 Hohe Daten-Durchsatzrate

Je nach Art der Verwendung und Nutzungsgrad der Schnittstelle können die Performance-Anforderungen an das System steigen: Übertragungsgeschwindigkeiten (Line Speed) zwischen 100 Mbit/s und 1 Gbit/s sowie der Durchsatz großer Datenmengen im Bulktransfer sollen realisierbar sein.

4.1.4 Automatischer Betrieb

Im ordnungsgemäßen Betrieb benötigt das System keine Eingriffe des Betreibers. Der Datentransfer erfolgt mit den Standardprotokollen SMTP (Mail), FTP (Dateitransfer) sowie TCP-Stream oder UDP-Datagram.

4.2 Sicherheitsanforderungen

Der Abfluss von Information aus dem roten ins schwarze Netz muss ausgeschlossen werden. Das System ermöglicht außerdem SMTP-Filterung auf Viren und Malware. Darüber hinaus sollen geeignete Verfahren zur Vermeidung von Covert Channel-Angriffen verfügbar sein.

5 Die Lösung: Die vs-diode

Anhand dieses Anforderungskatalogs hat genua ein hochsicheres Komplettsystem entwickelt, das auf der zertifizierten Firewall genugate und dem Microkernel L4 basiert. Die dreistufige vs-diode besteht aus einem One-Way-Filter, der sich zwischen zwei Application-Level-Gateways befindet.

5.1 Architektur mit drei separaten Filtersystemen

Die Architektur der vs-diode besteht aus der Abfolge der Subsysteme Application-Level-Gateway (ALG) – One-Way-Filter – Application-Level-Gateway, die die Daten auf ihrem Weg durch die Datendiode durchlaufen müssen.

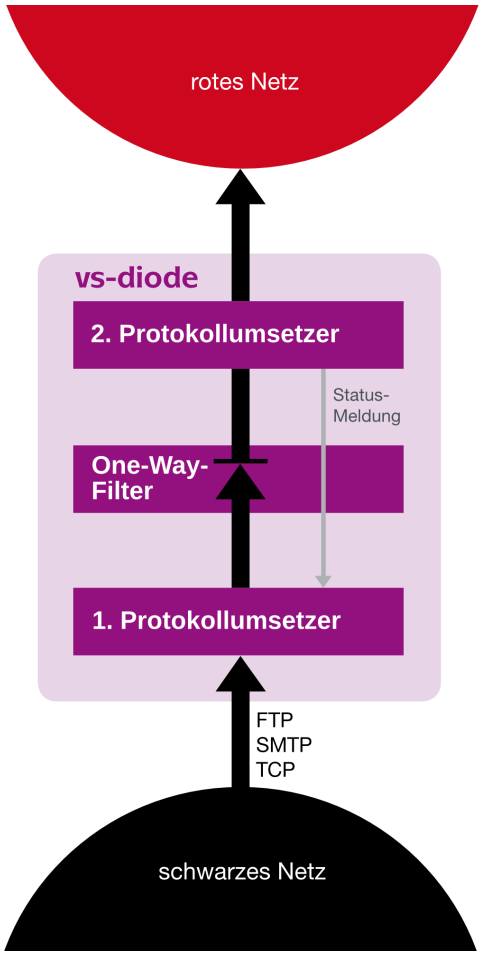

Abb. 2: vs-diode, bestehend aus einem One-Way-Filter und zwei Protokollumsetzern

Die drei separaten Komponenten der vs-diode funktionieren dabei zusammen wie eine Schleuse mit einem breiten und einem verengten Kanal: Daten aus dem schwarzen Netz werden angenommen und über eine neue Verbindung zum roten Netz transferiert, in umgekehrter Richtung darf dagegen lediglich eine Statusmeldung passieren.

5.2 Die Komponenten der vs-diode und ihre Funktion

Die Sicherheit der vs-diode rührt daher, dass verschiedene Technologien hintereinander geschaltet werden. Das sieht man bereits an der Hardware, die aus drei Teilen mit unterschiedlicher Implementierung besteht.

Basierend auf dem oben skizzierten Aufbau erhalten Sie nachfolgend einen tieferen Einblick in die einzelnen Komponenten und Prozesse der vs-diode.

5.2.1 Die Application-Level-Gateways (ALGs)

Die beiden ALGs sind zur Transformation komplexer Internetprotokolle auf einfach zu prüfende Einwegdatenströme zuständig. Die vs-diode unterstützt die Protokolle FTP, SMTP, TCP, UDP sowie Syslog und Lumberjack. Dadurch lassen sich Dateien und E-Mails übertragen, zudem können Logeinträge in Elasticsearch aggregiert werden. Dabei werden die Daten auf der schwarzen Seite angenommen und mit demselben Protokoll auf der roten Seite ausgeliefert. Die eingesetzten ALGs sind identisch mit denen der High Resistance Firewall genugate. Hier kommt bewährte und BSI-zertifizierte Technologie zur Inhalts- und Protokollanalyse zum Einsatz.

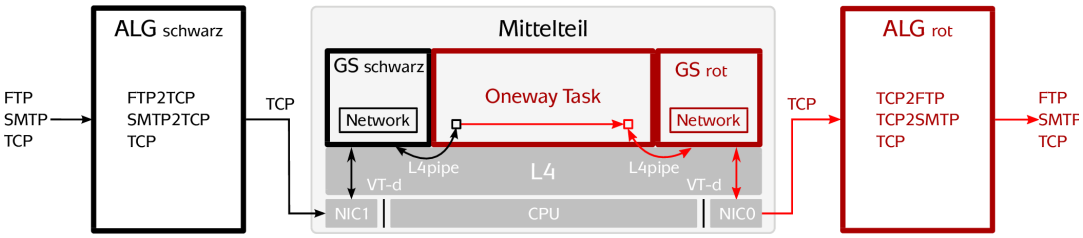

Abb. 3: Der Kommunikationsprozess im Überblick

Die Kommunikation über den Mittelteil der vs-diode (One-Way-Filter) hinweg erfolgt mittels TCP, welches nur von Schwarz nach Rot aufgebaut werden darf. Die Richtung des Datenflusses wird von den ALGs und vom One-Way-Filter auf eine Richtung beschränkt. Pro Verbindung ist ein Bit Rückkanal möglich, ein Fehler wird durch ein Reset-Paket des TCP-Protokolls signalisiert. Wenn etwa der Empfänger die Daten nicht annehmen kann, wird dieser Fehler durch ein Reset-Paket des TCP-Protokolls signalisiert.

5.2.2 Der One-Way-Filter

Um auch in den Steuerpaketen des TCP keine Informationen von Rot nach Schwarz verstecken zu können, wird die Verbindung im One-Way-Filter nochmals terminiert, umgewandelt und neu aufgebaut. Da TCP ein komplexes Protokoll ist, findet im One-Way-Filter eine weitere Trennung der Aufgaben statt.

Dazu nutzt genua einen Microkernel der L4-Familie. Dieser trennt die Hardware des One-Way-Filters in drei Compartments, also strikt getrennte Bereiche. Deren Aufgaben sind Annehmen der TCP-Verbindung, Überprüfen des Datenflusses und Aufbauen einer neuen TCP-Verbindung.

In den beiden Compartments, die sich um TCP kümmern, läuft jeweils eine Firewall und VPN-Appliance genuscreen. Obwohl wir diesem Produkt vertrauen, haben wir den Kernel auf der vs-diode als L4-Task paravirtualisiert und auf einen eigenen CPU-Kern und einen Teil des Hauptspeichers begrenzt. Wir verwenden die Virtualisierungstechnologie VT-d von Intel, um auch die Netzwerkhardware an diese Compartments zu koppeln. Die beiden Schwarz und Rot gekennzeichneten Interfaces sind mit den jeweiligen roten und schwarzen genuscreen-Compartments so fest gekoppelt, dass selbst Fehler in der Firmware der Netzwerkkarten oder in den Treibern ein Ausbrechen aus den Compartments unmöglich macht.

5.2.3 Der One-Way-Task

Zwischen den beiden genuscreens befindet sich ein One-Way-Task. Dieser wird durch den L4-Microkernel ebenfalls vom restlichen System entkoppelt. Der One-Way-Task kümmert sich ausschließlich darum, Daten von Schwarz nach Rot zu kopieren und eine Meldung über den Erfolg in umgekehrter Richtung zu erlauben. Da diese Aufgabe relativ einfach ist, lässt ich die Implementierung leicht überblicken. Das verhindert Fehler in dieser kritischen Komponente. Ein Verlust oder eine Verfälschung von Daten ist auf dieser Ebene nicht möglich.

5.2.4 Systemsicherheit

Wenn man den verschachtelten Systemaufbau betrachtet, muss man sich fragen, welche Komponenten letztlich für die Sicherheit unerlässlich sind. Die drei Maschinen ALG – One-Way-Filter – ALG sind hintereinander geschaltet und so konzipiert, dass die Nutzdaten nur in eine Richtung fließen. Auch beim Mittelteil besteht eine Dreiteilung in die Compartments genuscreen – One-Way-Task – genuscreen, welche alle für sich die Schutzziele erfüllen. Für die sichere Diodenfunktion ist es bereits ausreichend, dass nur der One-Way-Task und die L4-Separation nicht kompromittiert werden.

Der One-Way-Task ist mit etwa 1.300 Zeilen Code sehr übersichtlich. Der L4-Microkernel ist mit 38.000 Zeilen zwar schon deutlich größer, im Vergleich zu den üblichen Betriebssystemen mit mehreren Millionen Zeilen Code jedoch überschaubar. Dies gelingt dadurch, dass Hardwaretreiber und Netzwerkstack in den Compartments der genuscreen gekapselt werden. Diese gehören damit nicht mehr zur trusted Code-Base.

Selbst im unwahrscheinlichen Falle, dass das ALG der genugate, der Kernel der genuscreen oder die Firmware der Netzwerkkarten kompromittiert werden und es einen Innentäter gibt, der Daten über die Diode von Rot nach Schwarz transferieren möchte, werden der L4-Microkernel und der One-Way-Task dies zuverlässig verhindern.

5.2.5 Datenübertragung mittels FTP und SMTP

Die Annahme jedes FTP- und SMPT-Kommandos und der Daten erfolgt durch das ALG im schwarzen Netz. Das SMPT-Relay auf dem schwarzen ALG kann bestimmte MIME-Typen bzw. Dateiendungen überprüfen und gegebenenfalls filtern. Die Einbindung eines Virenscanners ist an dieser Stelle ebenfalls möglich. Nach erfolgreicher Prüfung werden die Daten an ein FTP2TCP-Relay übergeben.


Das FTP2TCP-Relay überträgt jedes Kommando über den One-Way-Filter mittels einer eigenen TCP-Verbindung an den entsprechenden Partnerprozess – das TCP2FTP-Relay auf dem roten ALG. Dabei werden die Daten per TCP-Stream übertragen, in Gegenrichtung wird nur Erfolg oder Misserfolg signalisiert.

Im roten Bereich werden dann aus den Daten dieser TCP-Verbindung das Kommando und die Daten restauriert. Das rote TCP2FTP-Relay leitet das Kommando an den FTP-Server weiter. Der Server schickt eine Statusmeldung, welche vom TCP2FTP-Relay auf erfolgreich/nicht erfolgreich untersucht wird.

5.2.6 Native Nutzung von TCP-Streams und UDP-Datagrams

Die Übertragung von TCP-Streams oder UDP-Datagrams vom schwarzen ins rote Netz stellt eine weitere Option dar. Dabei werden bei TCP dem Client im schwarzen Netz entsprechende Informationen zurückgegeben, die über den Erfolg/Misserfolg des Transfers informieren. Dadurch bietet das TCP-Protokoll eine hohe Zuverlässigkeit, während es bei UDP selbst bei mehrfacher Übertragung keine Garantie für den Empfang der gesendeten Pakete gibt, da die Daten protokollbedingt nur in eine Richtung fließen.

5.3 Die Sicherheitsmerkmale der vs-diode im Überblick

Der Übertragungsprozess innerhalb der vs-diode ist durch zahlreiche Sicherheitsvorkehrungen gekennzeichnet.

5.3.1 Trennung des TCP-Datenstroms an beiden ALGs

Der TCP-Datenstrom wird an beiden ALGs unterbrochen und die Informationen werden zwischengelagert – eine Weiterleitung von Paketen findet nicht statt. Bei dem erneuten Verbindungsaufbau werden sämtliche Kontrollinformationen wieder zurückgesetzt. Somit enthalten die Header der übertragenen TCP-Pakete nur die zur Kommunikation erforderlichen Daten und sind frei von jeglichen Inhalten. Ein unbeabsichtigter Informationsfluss von Rot nach Schwarz sowie Timing- und Covert Channel-Angriffe sind somit auf dieser Ebene ausgeschlossen.

5.3.2 Content-Filterung für SMTP und FTP möglich

Je nach eingesetztem Protokoll bietet die vs-diode verschiedene Filtermöglichkeiten: Das SMTP-Relay auf dem schwarzen ALG ist in der Lage, Parameter eintreffender Mails wie Mail-Berechtigung des Absenders, MIME-Typen, Dateiendungen, Script-Sprachen und aktive Inhalte anhand bestimmter Regeln zu überprüfen und den Mail-Empfang gegebenenfalls zu verweigern. Das FTP-Relay auf dem schwarzen ALG kann bestimmte Anfragemethoden überprüfen und entsprechend filtern.

5.3.3 Einsatz von Virenscannern möglich

Durch Virenscanning auf dem schwarzen ALG kann das sensible rote Netz zuverlässig vor schädlichem Code geschützt werden.

Dazu bearbeitet die optionale Zusatzsoftware genuscan die eintreffenden Daten in einem so genannten Cage, einem abgesicherten Bereich im Dateisystem des ALG. Die Daten

werden dort für den Virenscanner aufbereitet, indem sie gegebenenfalls dekomprimiert und Archive in einzelne Dateien zerlegt werden. Diese Aufbereitung wird – sofern nötig – auch rekursiv durchgeführt.

Wenn der Scanner Viren entdeckt, initiiert genuscan entsprechende Alarmmeldungen. Die virenbefallenen E-Mails werden von genuscan im abgesicherten Bereich zurückgehalten und können dort einer weiteren Analyse unterzogen werden. Nur Daten, in denen keine Viren gefunden wurden, leitet genuscan an die zustellende Applikation weiter. genuscan arbeitet mit dem Virenscanner Antivir Professional zusammen.

5.3.4 Hochsichere Diodenfunktion des One-Way-Filters

Die komplexen Prüfungsroutinen der beiden ALGs werden um einen One-Way-Filter ergänzt. Er bildet als separate Appliance den Mittelteil und beinhaltet die wesentliche Sicherheitskomponente der vs-diode. Der One-Way-Filter lässt eine Informationsübertragung nur von Schwarz nach Rot zu. Die eigentliche Diodenfunktion ist auf einem minimalistischen Microkernel-System implementiert. Sie ist von geringer Komplexität und einfach zu analysieren. Ihr kompletter Code kann überprüft werden, um Fehler in dieser entscheidenden Komponente auszuschließen. Die hochsichere Diodenfunktion ist das zentrale Merkmal der vs-diode und garantiert absolut zuverlässige Einbahn-Datentransfers.

5.3.5 Hochsicherer Bootvorgang des One-Way-Filters

Gebootet wird der One-Way-Filter mittels einer speziell entwickelten Coreboot-Implementierung, die als minimales BIOS nur erlaubte Hardware-Komponenten initialisiert. Eine Erweiterung um die UEFI Secure Boot-Funktionalität ermöglicht ausschließlich das Laden von Software, die von genua signiert ist. Fremdsoftware oder ein verändertes Betriebssystem kann somit nicht geladen werden.

5.3.6 Fremdzugriff auf Bootmedium ausgeschlossen

Beim Bootmedium des One-Way-Filters handelt es sich um eine CD-ROM mit statischer Konfiguration. Diese folgt dem Security by Design-Ansatz: Die Informationsübertragung durch den One-Way-Filter nur von Schwarz nach Rot kann weder mit Absicht noch durch Konfigurationsfehler verändert werden. Erlaubte Änderungen wie Updates oder Upgrades erfordern physischen Zugriff auf das Gerät. Dadurch ist die Sicherheit des Systems wesentlich erhöht.

5.3.7 Härtung der ALGs

Das auf den ALGs eingesetzte Betriebssystem OpenBSD ist gegen Angriffe gehärtet und damit für den Einsatz in einer Datendiode optimiert.

5.4 Performance

Die vs-diode bietet als Einzelsystem einen Datendurchsatz von bis zu 1 Gbit/s, der durch Load-Sharing mittels Cluster-Bildung beliebig erweiterbar ist (ab einem folgenden Release verfügbar).

5.4.1 Hardware

Die vs-diode bieten wir momentan in der Hardware-Variante M an. Da genua die Ausstattung der Hardware-Varianten (z. B. den CPU-Typ) laufend der technischen Entwicklung anpasst, unterliegen diese Daten steten Veränderungen. Die aktuelle technische Ausstattung können Sie unserem Hardware-Datenblatt entnehmen.

5.4.2 Hochverfügbarkeit durch Cluster

Für viele Organisationen ist die ständige Verfügbarkeit der Sicherheitssysteme absolut notwendig. Dafür stellt genua Cluster-Lösungen bereit, die aus mehreren vs-dioden bestehen (ab einem folgenden Release verfügbar).

Diese Lösung hat folgende Vorteile:

- Alle für die Hochverfügbarkeit eingesetzten Systeme teilen sich im Normalbetrieb die Aufgaben.
- Ein manuelles Eingreifen beim Ausfall eines Systems ist nicht notwendig.
- Der Cluster kann beliebig erweitert werden, um hinsichtlich der Bandbreite höhere Anforderungen zu erfüllen (Skalierbarkeit).

6 Einsatzszenarien

Naheliegend ist der Einsatz der vs-diode aufgrund der unter Punkt 3 genannten Vorschriften in Behörden und im Bereich der militärischen Kommunikation. Darüber hinaus ist sie zur Absicherung von Netzen geeignet, die mit Forschungslabors, Entwicklungsabteilungen oder weiteren sensitiven Segmenten der Privatwirtschaft in Zusammenhang stehen.

Besonders strikte Sicherheitsregeln gelten im militärischen Bereich, da die Landesverteidigung zu den vitalen Interessen eines Staates gehört: Eingestufte Daten wie etwa Lageberichte, Befehle oder Informationen über moderne Waffensysteme müssen nach den Vorgaben des Geheimschutzes behandelt werden. Solche Daten sind ausschließlich in den besonders geschützten roten Netzen zu bearbeiten und dürfen keinesfalls in schwarze Netze übertragen werden.

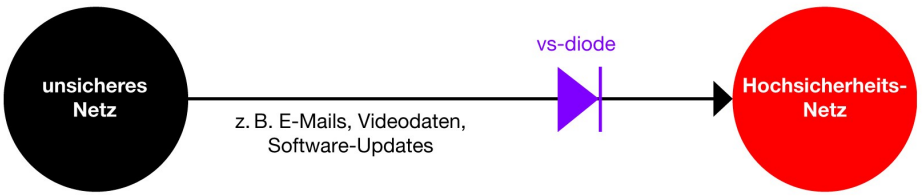

Abb. 4: One Way-Datentransfer in ein Hochsicherheitsnetz

Niedriger eingestufte oder allgemein verfügbare Daten, die auch für Planungssysteme in roten Netzen relevant sind, sollen hingegen von schwarzen in rote Netze übertragen werden können.

Alle aus dem roten Netz stammenden Daten sind somit nach außen abzusichern, damit keine vertraulichen Informationen in unbefugte Hände gelangen. In umgekehrter Richtung – vom schwarzen ins rote Netz – sollen die Firewalls zwar den Datentransfer erlauben, jedoch Viren und Schad-Software herausfiltern.

Für dieses Einsatzgebiet ist die vs-diode konzipiert: Neben einer umfassenden Überprüfung der zu übertragenden Daten bietet sie einen vollständig automatisierten, unidirektionalen Echtzeit-Informationstransfer im 24/7-Betrieb. Darüber hinaus erfüllt sie die hohen Anforderungen, die mit einer militärischen Nutzung einhergehen – sowohl stationär als auch an Bord von Schiffen.

Konkrete Anwendungsbeispiele im staatlichen wie im privatwirtschaftlichen Bereich sind Geo-Informationssysteme (GIS), Enterprise Resource Planning-Systeme (ERP) und Steuernetze großtechnischer Anlagen – z. B. für Kernkraftwerke oder Stellwerksysteme von Bahngesellschaften – die aus Sicherheitsgründen in rote Netze einbezogen und gleichzeitig auf einen laufenden Datenabgleich angewiesen sind.

Die Unterstützung des Lumberjack-Protokolls ermöglicht die Aggregation, Analyse, Visualisierung und Weiterverarbeitung von Daten mit Elasticsearch-Anwendungen in abgeschotteten Netzen. Zu diesem Zweck können Daten aus verschiedenen Quellen über die vs-diode in eine zentrale Ablage übertragen und nach außen abgesichert werden. Durch die Einsatzmöglichkeit der vs-diode zwischen verschiedenen Datenablagen lassen sich darüber hinaus hierarchische Architekturen hochsicherer Instanzen zur Datenauswertung aufbauen.

Durch die FTP-Unterstützung ist die vs-diode auch zur Synchronisation großer Datenbestände geeignet.

Das System lässt sich individuellen Einsatzbereichen flexibel anpassen. Beispielsweise können zusätzliche Schutzmechanismen für das rote Netz gegen Malware oder aktive Inhalte realisiert werden.

7 Zulassung

Während ein Antrag auf Sicherheitszertifizierung eines IT-Produkts durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) vom jeweiligen Hersteller gestellt werden kann und der Qualitätssicherung dient, darf ein BSI-Zulassungsverfahren nur durch einen behördlichen Anwender (Bedarfsträger) beantragt werden.

Gegenstand eines solchen Zulassungsverfahrens sind ausschließlich IT-Sicherheitsprodukte, die für die Verarbeitung und Übertragung von amtlich geheimgehaltenen Informationen (Verschlusssachen) im Bereich des Bundes und der Länder oder bei Unternehmen im Rahmen von Aufträgen des Bundes oder der Länder eingesetzt werden.

Die vs-diode ist bis zur VS-Stufe GEHEIM zugelassen.

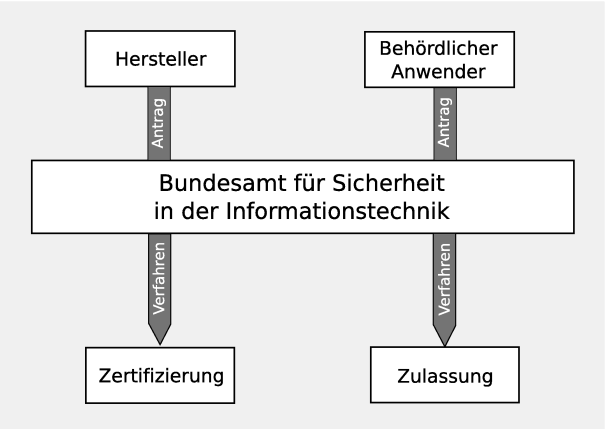

Abb. 5: Unterschiedliche Verfahren zur Zertifizierung und Zulassungen von IT-Produkten

Für weitere Informationen zu den Themen Zertifizierung und Zulassung nehmen Sie bitte Kontakt mit uns auf. Wir beraten Sie umfassend.

8 Support

8.1 Installations-Service

genua und spezialisierte Partner unterstützen Sie auf Wunsch bei der Installation, Konfiguration und Inbetriebnahme Ihrer vs-diode. Dabei werden die Administratoren ausführlich in die Benutzung und Pflege eingewiesen. Falls Sie es wünschen, erstellen wir Ihnen zuvor ein Feinkonzept für Ihre sichere Netzkopplung.

8.2 Schulungen

Bei genua erhalten Sie ein speziell auf Ihren Bedarf abgestimmtes Schulungsangebot. Genauere Informationen erhalten Sie auf Anfrage. Wir beraten Sie gerne.

8.3 Laufender Betrieb – Software Support

Update Service: Die Lösungen von genua werden ständig weiterentwickelt. Regelmäßig erscheinen neue Versionen, in denen aktuelle Entwicklungen aufgegriffen werden und der

Funktionsumfang sinnvoll ergänzt wird. Je nach Bedarf erscheinen zusätzlich Zwischenversionen.

Hotline: Zusätzlich zu unserem Update-Service bieten wir Support durch überprüfte Mitarbeiter (bis Ü2) via Telefon und E-Mail. Sie können unsere Hotline für alle Fragen zu Ihrer Lösung nutzen. Der telefonische Hotline-Support steht Ihnen auf Wunsch 24 Stunden an allen Tagen zur Verfügung. So können Sie sich jederzeit auf deutschsprachigen Support direkt vom Hersteller verlassen.

8.4 Laufender Betrieb – Hardware Support

Next Business Day Austausch-Service: Bei defekter Hardware erhält der Kunde innerhalb Deutschlands am nächsten Werktag ein baugleiches Gerät im Austausch für das defekte Gerät. Leistungsumfang und Voraussetzungen entnehmen Sie bitte den Allgemeinen Vertragsbedingungen der genua GmbH.

Service-Leistungen bei Kunden können durch überprüfte Mitarbeiter von genua (bis Ü3) erbracht werden.

So erreichen Sie uns:

genua GmbH, Domagkstraße 7, 85551 Kirchheim bei München
tel +49 89 991950-0, fax +49 89 991950-999, info@genua.de, www.genua.de

9 Glossar

ALG	Application-Level-Gateway: Firewall, die auf Anwendungsebene arbeitet. Ein ALG lässt keine direkte Kommunikation zwischen "innen" und "außen" zu. Es prüft die empfangenen Anwendungsdaten und kann z. B. nach Viren oder URLs scannen. ALGs sind vom Sicherheitsstandpunkt Paketfiltern deutlich überlegen, benötigen jedoch performantere Hardware.
CC	Common Criteria: Allgemeine Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik.
Covert Channel	Parasitärer Kommunikationskanal, der Bandbreite von einem legitimierten Kommunikationskanal benutzt, um Informationen zu übermitteln.
EAL	Evaluation Assurance Level – Prüftiefe im Rahmen einer CC-Zertifizierung.
FTP	File Transfer Protocol – Netzprotokoll zur Übertragung von Dateien über IP-Netzwerke.
FTP2TCP-Relay	Spezial-Relay der Datendiode, setzt FTP in einen unidirektionalen TCP-Strom um.
genugate	High Resistance Firewall bestehend aus ALG und PFL.
genuscreen	Stateful Packet Filter & VPN-Appliance.
L4	Mikrokernel, basierend auf Konzepten von Jochen Liedtke, der die Funktionsweise des One-Way-Filters hochsicher durchsetzt.
One-Way-Filter	Mittelteil der vs-diode, der die eigentliche Diodenfunktion bereitstellt.
Parser	Programm zur Zerlegung und Umwandlung einer beliebigen Eingabe in ein für die Weiterverarbeitung brauchbares Format.
Relay	Implementierung eines protokollspezifischen Proxies auf einem genugate-Firewall-System.
SMTP	Simple Mail Transfer Protocol – Netzprotokoll, das zum Austausch von E-Mails in Computernetzen dient.

SMTP2TCP	Spezial-Relay der Datendiode, setzt SMTP in einen unidirektionalen TCP-Strom um.
TCP	Transmission Control Protocol – Netzprotokoll für eine zuverlässige Übertragung, die verbindungs- und stromorientiert ist.
TCP2FTP	Spezial-Relay der Datendiode, stellt das Pendant zum FTP2TCP-Relay dar und setzt TCP in FTP um.
TCP2SMTP	Spezial-Relay der Datendiode, stellt das Pendant zum SMTP2TCP-Relay dar und setzt TCP in SMTP um.
UDP	User Datagram Protocol – Minimales Netzprotokoll, das einen verbindungslosen, nicht-zuverlässigen Übertragungsdienst bereitstellt.
VSA	Verschlusssachenanordnung: Allg. Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen.