

Sicherheits-Gateways für Rot-Schwarz-Übergänge

Von Dr. Magnus Harlander

Wer stets ein aktuelles Bild der Lage hat, ist klar im Vorteil. Dafür sind ein ständiger Datenaustausch und eine umfassende Vernetzung erforderlich. Aber im militärischen Bereich gelten für den Datenfluss strikte Grenzen. Viele Informationen sind eingestuft – sie müssen nach den Vorgaben der Verschlusssachenanordnung (VSA) behandelt werden. Eingestufte Informationen sind ausschließlich in den besonders geschützten roten Netzen zu bearbeiten und dürfen nicht in schwarze Netze übertragen werden, da hier deutlich geringere Sicherheitsanforderungen gelten. An den Übergängen – den Rot-Schwarz-Schnittstellen – muss also eine strikte Kontrolle stattfinden: Während Daten ungehindert von Schwarz nach Rot fließen dürfen, sind Transfers in Gegenrichtung zu unterbinden oder es muss sichergestellt werden, dass ausschließlich freigegebene Informationen den Übergang passieren. Dazu muss hier der Inhalt der Daten kontrolliert werden. Diese Aufgabe ist mit herkömmlichen Firewalls nicht zu lösen – hier müssen spezielle Sicherheits-Gateways eingesetzt werden.

VSA-ingestufte Dokumente dürfen auf keinen Fall in unautorisierte Hände gelangen. Es ist laut VSA davon auszugehen, dass die „Kenntnisnahme eines geheim eingestuftes Dokuments durch Unbefugte die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährden oder ihren Interessen schweren Schaden zufügen kann.“ Der Gesetzgeber hat hier also eine Formulierung gewählt, die ein stark ausgebildetes Bewusstsein für die vertrauenswürdige Behandlung von eingestuftem Material fordert. Verstöße gegen die VSA sind für die Verantwortlichen mit strafrechtlichen Konsequenzen bedroht.

Werden Netze unterschiedlicher Einstufungen miteinander verbunden, spricht man von einem Rot-Schwarz-Übergang und die VSA verlangt hier den Einsatz spezieller Gateways, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zugelassen sein müssen. Diese Systeme unterscheiden sich grundsätzlich von herkömmlichen Firewalls und sollen zweifelsfrei sicherstellen, dass keine höher eingestuftes roten Daten in niedriger eingestufte schwarze Netzwerke gelangen können. Bei der Zulassung wird ausführlich geprüft, ob die Systeme diese Anforderung tatsächlich unter allen Umständen erfüllen.

Bedrohungen und Maßnahmen zur Abwehr

Angesichts der weitreichenden Konsequenzen eines Fehlverhaltens bei diesen Übergängen sind erhebliche Anstrengungen notwendig, um den Abfluss von eingestuftem Material zu verhindern. Man hat dabei davon auszugehen, dass so ziemlich alles schief geht, was schief gehen kann und bezieht das in die Bedrohungsanalyse mit ein. Die für diesen Einsatz zugelassenen Systeme müssen gegen all diese

Bedrohungen resistent sein und sie zuverlässig entschärfen. Man denkt dabei vor allem an folgende – nicht wirklich unwahrscheinliche – Szenarien:

- Die auf den Gateways eingesetzte Software hat Fehler.
- Die Gateway-Systeme sind falsch konfiguriert worden.
- Die Konfiguration der Gateway-Systeme wurde nachträglich durch das Betriebspersonal geändert.
- Die aktuelle Konfiguration entspricht nicht dem notwendigen Schutzbedarf. Gründe hierfür können mangelndes Wissen, Unachtsamkeit oder auch Fahrlässigkeit sein.
- Die Systeme wurden in einen intermediären Zustand gebracht, der nicht die vollständige Umsetzung der Konfigurationseinstellung mit sich bringt.
- Auf der roten Seite des Netzes wird ein Datentransfer versehentlich oder bewusst, d. h. durch einen Innentäter, Richtung schwarzes Netz angestoßen.

In Rot-Schwarz-Gateways werden daher Sicherheitsfunktionen eingebaut, die die oben genannten Bedrohungen weitgehend entschärfen sollen.

Sicherheitsfunktionen

Redundanz: Durch Redundanz für Sicherheitsfunktionen kann man verhindern, dass beim Ausfall einer Funktion das ganze System durchlässig wird. Der Ausfall einer Sicherheitsfunktion kann durch einen Fehler in der Software oder in der Bedienung geschehen – und dies tritt immer wieder auf. Auch bei normalen Firewall-Systemen sollte dieses Prinzip beachtet werden. Bei Rot-Schwarz-Gateways ist es unabdingbar.

Unabhängigkeit: Die Implementierung von verschiedenen Sicherheitsfunktionen sollte weitgehend voneinander isoliert sein. Wird eine Funktion überwunden, z. B. durch einen Root-Exploit, darf das nicht dazu führen, dass auch die anderen ausgehebelt werden können. Daher werden in Rot-Schwarz-Gateways oft mehrere unabhängige Systeme miteinander kombiniert und die Sicherheitsfunktionen auf diese verteilt. Diese Art von Mehrfachabsicherung erfüllt natürlich auch das oben genannte Redundanzprinzip.

Konfigurationskontrolle: Die Konfiguration eines Gateways bestimmt, was es durchlässt und was nicht. Daher darf diese nicht mehr beliebig veränderbar sein – sie muss erzwungen werden können. Dies kann konstruktionsbedingt geschehen oder durch besondere operative Maßnahmen erreicht werden, wie z. B. ein Vier-Augenprinzip bei der Konfigurationserstellung, Nutzung von digitalen Signaturen oder einer Offline-Generierung der Konfiguration.

Inhaltskontrolle: Werden Daten wirklich von Rot nach Schwarz transportiert, darf man sich nicht nur mit der Kontrolle und Überprüfung der Protokollelemente begnügen, sondern muss die Daten vollständig auf Byte-Ebene kontrollieren. Es muss sichergestellt sein, dass nur Daten den roten Bereich verlassen, die das auch dürfen.

Sicherheits-Gateways für Rot-Schwarz-Übergänge

Rot-Schwarz-Übergänge können mit zwei unterschiedlichen Klassen von Sicherheits-Gateways realisiert werden, die beide die TCP/IP-Protokollfamilie nutzen: One-Way-Gateways und bidirektionalen Gateways.

One-Way-Gateways: One-Way-Gateways sind Dioden, die eingesetzt werden, wenn nur ein Datentransfer vom schwarzen in das rote Netz benötigt wird. Es wird hier konstruktionsbedingt gewährleistet, dass Daten nur von Schwarz nach Rot fließen können. Dabei ist sicherzustellen, dass die in den roten Bereich transferierten Daten nicht von bösartiger Natur sind, aber man muss sich immerhin keine Gedanken über den Rückweg machen. Dieser ist schließlich per Konstruktion ausgeschlossen und kann auch nicht versehentlich aktiv werden. Bei den Dioden gibt es zwei unterschiedliche Ansätze:

Paketdioden: Diese Systeme können nur einzelne IP-Pakete in der Richtung von Schwarz nach Rot transferieren. Denn die Rückrichtung ist grundsätzlich unterbunden – wenn es richtig gemacht ist, nicht per Software, sondern per Hardware. Die einfachste Methode ist eine einfasige Glasfaser zu verwenden und die Sendee- und Empfangssysteme so anzupassen, dass sie mit dieser Situation zurechtkommen.

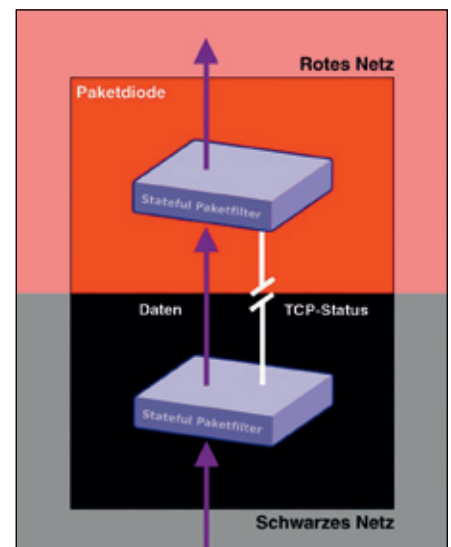


Bild 1: Paketdiode ermöglicht nur Datentransfer von Schwarz nach Rot

Bild 1 stellt eine solche Konstellation dar. Der Vorteil einer Paketdiode ist das einzigartig hohe Sicherheitsniveau. Da kein Rückweg existiert, kann er auch nicht benutzt werden. Der Nachteil: Diese Systeme sind nur einsetzbar, wenn kein Feedback über die gesendeten Daten benötigt wird. Transfers größerer zusammenhängender Datenmengen wie Dateien sind so fast unmöglich, da keine Bestätigung über den Empfang der einzelnen Pakete erfolgt und daher unklar bleibt, ob die Daten auch wirklich vollständig angekommen sind. Für die schnelle Übermittlung von kleinen Datenpaketen wie z. B. Statusmeldungen und Lagedaten sind diese Dioden aber gut geeignet.

Datendiode: Bei vielen Anwendungen ist aber sicherzustellen, dass die gesendeten Daten wirklich angekommen sind. Hier muss ein Protokoll eingesetzt werden, das Feedback-Möglichkeiten und Flow-Control bietet. Somit ist eine physikalische Rückverbindung zwingend erforderlich. Diese könnte Out-Of-Band z. B. über eine serielle Schnittstelle realisiert werden. Sie kann aber auch, wenn man große Sorgfalt walten lässt, mit einem TCP-basierten System realisiert werden.

Bild 2 stellt eine mögliche Konstellation einer TCP-Datendiode vor, in der die Diodenfunktion durch einen Paketfilter realisiert ist, der Daten nur in eine Richtung passieren lässt, TCP-Status-Informationen hingegen in beide Richtungen. Dabei muss verhindert werden, dass in den TCP-Status-Informationen versteckte Informationen übertragen werden, also in den IP- und TCP-Headern. Deshalb werden die TCP-Verbindungen durch Application Level Gateways terminiert, die Teil der Datendiode sind. Diese Systeme realisieren auch die Protokollumsetzung von z. B. SMTP auf ein One-Way-Protokoll.

Der Vorteil einer solchen Datendiode liegt auf der Hand: Sie kann auch große Datenmengen schnell und zuverlässig übertragen, garantiert aber dennoch ein sehr hohes Maß an Sicherheit, da die drei beteiligten unabhängigen Systeme den Rückfluss von Daten auf dem Feedback-Kanal verhindern.

Bidirektionale Gateways: Wenn Daten in beide Richtungen transferiert werden sollen, müssen ganz andere Systemarchitekturen betrachtet werden. Der Schutz des roten Netzes vor böswilligen Daten bei Übertragung von Schwarz nach Rot ist natürlich auch hier sicherzustellen, aber dafür können klassische Filtersysteme wie Firewalls und Virens Scanner eingesetzt werden. Die anspruchsvollere Aufgabe aber ist der sichere Rückweg. Hier dürfen nur Daten transferiert werden, die dafür vorgesehen sind. Es muss eine Freigabe durch eine berechtigte Person oder ein einsprechend autorisiertes System erfolgen.

Manuelle Freigabe: Die Prüfung für die Freigabe kann manuell durch Inspektion der Daten mit einem zuverlässigen Viewer geschehen, wonach Daten zur Übertragung durch eine Person freigegeben werden. Die Freigabe kann z. B. durch die Erstellung einer digitalen Signatur geschehen, die auf dem Gateway-System überprüft werden kann. Dieser Prozess ist natürlich nur auf prüfbare Dokumente be-

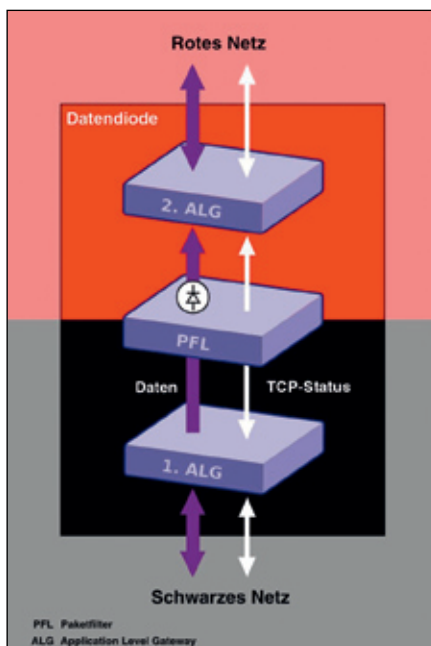


Bild 2: Datendiode ermöglicht schnellen und zuverlässigen Schwarz-Rot-Transfer

schränkt, was z. B. PDF oder Microsoft-Word als Format ausschließt, da hier versteckte Informationen mitübertragen werden könnten. Es lässt sich aber immerhin z. B. RTF als weiterverarbeitbares Format zuverlässig darstellen und freigeben.

Automatische Freigabe: Soll der Prozess der Freigabe automatisiert ablaufen, müssen die zu prüfenden Daten in einem automatisch prüfbares Format vorliegen. Das kann z. B. XML oder ein anderes automatisch parsebares Format sein. Ein Automat vermag aber nicht zu beurteilen, ob eine beliebige Textinformation freigegeben werden kann. Mit diesem Verfahren lassen sich also keine Freitexte prüfen, wohl aber maschinenlesbare und -verarbeitbare Daten wie z. B. Statusinformationen, Zahlen, Koordinaten oder auch zuvor festgelegte Textelemente.

Mit einer automatischen Freigabe können z. B. elektronische Prozesse wie eine Datenbank-Synchronisation über eine Rot-Schwarz-Schnittstelle hinweg durchgeführt werden, wobei das Ergebnis der Transaktion – Fehler oder Erfolg – zurückgemeldet wird. Ein anderes Verfahren wäre der Online-Zugriff auf eine schwarze GIS-Datenbank per Web Browser. Hier könnte ein roter Client Abfragen von Geo-Daten in einer schwarzen Datenbank absetzen. Beides sind Prozesse, die bisher gar nicht oder nur sehr mühsam und fehleranfällig in Offline-Verfahren realisierbar waren.

Sicherheitsgateway RSGate mit Zulassung bis GEHEIM

Die deutschen Sicherheitsunternehmen GENUA und INFODAS haben das Sicherheits-Gateway RSGate entwickelt, das den bidirektionalen Datenaustausch an Rot-Schwarz-Übergängen ermöglicht.

Bild 3 zeigt den Aufbau des Sicherheits-Gateways RSGate. Diese Lösung ist vom Bun-

desamt für Sicherheit in der Informationstechnik (BSI) für den Einsatz bis GEHEIM bei der Bundesmarine zugelassen und auf den neuen Fregatten F125 zur Absicherung sensibler Schnittstellen fest eingeplant.

Der Weg von Rot nach Schwarz

Das RSGate besteht aus den Komponenten Viewer, Sicherheitsfilter, zwei Firewalls zur Trennung der Netze und einem Data Store. Hier das Zusammenspiel der Komponenten beim Datentransfer per E-Mail vom roten zum schwarzen Netz:

- ➔ ① Roter Arbeitsplatz: Eine Datei für einen Empfänger im schwarzen Netz wird als E-Mail-Anhang gesendet.
- ➔ ② Viewer: Maschinell prüfbare Dateien werden voll automatisiert vom Parser kontrolliert, andere Formate manuell vom Anwender, der über den Viewer eine Freigabe erteilen kann. Falls keine vertraulichen Informationen enthalten sind, wird die Datei digital signiert und als E-Mail an die rote Firewall weitergeleitet.
- ➔ ③ Rote Firewall: Nimmt ausschließlich signierte E-Mails entgegen und leitet diese an den Sicherheitsfilter weiter.
- ➔ ④ Sicherheitsfilter: Prüft die Signatur. Falls diese korrekt und unverändert ist, wird die Datei an eine neue E-Mail angehängt und an die schwarze Firewall weitergeleitet.
- ➔ ⑤ Schwarze Firewall: Scant E-Mail inkl. Anhang und entfernt Viren sowie aktive Inhalte. Anschließend wird die E-Mail an den Empfänger weitergeleitet.
- ➔ ⑥ Schwarzer Arbeitsplatz: Die Datei trifft als E-Mail-Anhang beim Empfänger ein.
- ➔ ⑦ Data Store: Hier können mittels Viewer freigegebene Dateien abgelegt werden, um sie im gesamten schwarzen Netz zum Abruf per HTTP oder FTP bereitzustellen.

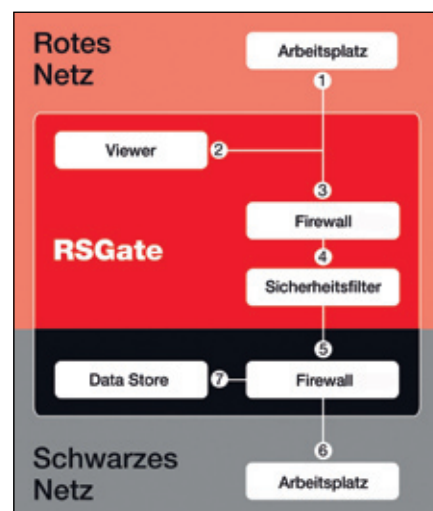


Bild 3: Sicherheits-Gateway RSGate ermöglicht Datentransfer in beide Richtungen

Dr. Magnus Harlander ist Geschäftsführer des IT-Sicherheitsunternehmens GENUA mbH in Kirchheim bei München.