SDoT Diode®

Sichere, unidirektionale Hochgeschwindigkeits-Datenübertragung zwischen Netzen mit unterschiedlichen Einstufungen

Grundlagen

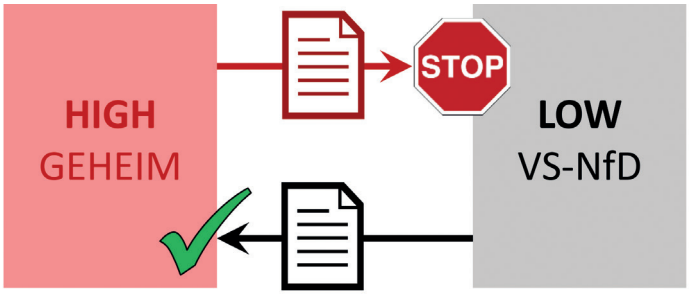
Moderne, militärische Führungsinformationssysteme und vergleichbare Systeme von zivilen Behörden nutzen Computernetze um Daten zu erfassen, verarbeiten und auszutauschen. Aufgrund der Einstufung der Daten („Verschlusssachen“) erfolgt die Verarbeitung in so genannten Sicherheitsdomänen. Solche Sicherheitsdomänen haben üblicherweise keine Verbindung zu anderen Sicherheitsdomänen, insbesondere wenn in ihnen GEHEIM oder vergleichbar eingestufte Daten verarbeitet werden. Der Schutz der sensitiven Informationen innerhalb der Sicherheitsdomänen hat höchste Priorität und wird regelmäßig durch strikt voneinander getrennte Computernetze realisiert.

Bedarf an Datenaustausch

Ein Datenaustausch zwischen den unterschiedlichen Sicherheitsdomänen ist dennoch notwendig. Die in getrennten Netzen arbeitenden Behörden müssen untereinander und auch übergreifend Informationen austauschen um ihre jeweiligen Aufträge zu erfüllen. Eine Datenübertragung zwischen Sicherheitsdomänen mit unterschiedlichen maximal verarbeiteten Geheimhaltungsgraden ist nur unter Einhaltung hoher Sicherheitsstandards möglich und erlaubt. Aus Geheimschutzsicht ist die Übertragung von Daten aus einem niedrig klassifizierten Netz („LOW“, z. B. VS-NfD) in ein höher klassifiziertes Netz („HIGH“, z.B. GEHEIM) problemfrei, da alle in LOW existierenden Daten auch in HIGH verarbeitet werden dürfen. Es muss allerdings unbedingt sichergestellt werden, dass in der Gegenrichtung absolut keine Informationen übertragen werden. Aufgrund der bidirektionalen Auslegung der in Computernetzen verwendeten IP-Protokolle kann die Kopplung unterschiedlicher Domänen nur mit einem so genannten Gateway erfolgen.

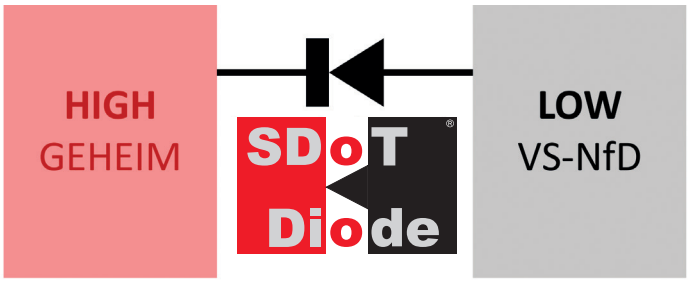
Die SDoT Diode®

Das Produkt „Secure Domain Transition **SDoT Diode®**“ der INFODAS GmbH verbindet unterschiedlich klassifizierte Netze und ermöglicht einen Datentransfer in ausschließlich einer einzigen Richtung – von LOW nach HIGH:



Erlaubte und verbotene Datenübertragung

Jede andere Form des Datenaustauschs – auch auf niedriger Ebene der Kommunikationsprotokolle – wird unterbunden, um sicher zu gehen, dass absolut keine Informationen und Daten die höher klassifizierte Domäne verlassen.
Die **SDoT Diode®** ist somit ein strikt unidirektionales Gateway:



Die **SDoT Diode®** verbindet Sicherheitsdomänen

Besteht Bedarf an einer bidirektionalen Kommunikation, sollen also insbesondere bestimmte Informationen nach einer inhaltlichen Kontrolle doch von HIGH nach LOW fließen können, so steht statt der **SDoT Diode®** das Produkt **SDoT Security Gateway®** zur Verfügung.

Performante Datenübertragung

Eine Datendiode kann auf eine strikte inhaltliche Kontrolle der zu übertragenden Daten verzichten. Sie sorgt vielmehr dafür, dass die Daten ausschließlich in einer einzigen Richtung transportiert werden. Deshalb ist die **SDoT Diode®** sehr schnell und erreicht nahezu die Bandbreite der zugrundeliegenden Netzwerkinfrastruktur. Um die maximale Performance zu gewährleisten, ist die **SDoT Diode®** mit zwei leistungsstarken 10 Gbit/s-Netzwerkschnittstellen ausgestattet. Die **SDoT Diode®** ist damit hervorragend geeignet, um große Datenmengen in kurzer Zeit aus einer LOW-Domäne in eine HIGH-Domäne zu transportieren. Auch die Latenz ist so gering, dass Echtzeitanwendungen möglich sind. Mit der **SDoT Diode®** können die unsicheren, berüchtigten „Drehstuhlschnittstellen“ gegen eine hocheffiziente und sichere Übertragung ausgetauscht werden.

Sicherheitsarchitektur

Die **SDoT Diode®** nutzt eine Sicherheitsarchitektur, die auf dem neuen Microkernel-Betriebssystem der INFODAS GmbH mit starker Separierung aufsetzt. Die sicherheitskritischen Funktionen der **SDoT Diode®** werden durch so genannte „Kompartments“ wirksam und nachweisbar von den nicht-sicherheitskritischen Funktionen abgeriegelt.
Durch die Separierungsfunktionen des Betriebssystems werden unter anderem die Netzwerkschnittstellen zu beiden Netzen wirksam voneinander getrennt. Ein Direktzugriff eines potenziellen Angreifers aus dem LOW-Netz in das HIGH-Netz wird effektiv unterbunden.
Das Betriebssystem verfügt als Microkernel über eine stark minimalisierte Anzahl von Programmcode. Dieser reduzierte Umfang macht eine Evaluierung erst möglich, da übliche Betriebssysteme sehr umfangreich und damit unter wirtschaftlichen und zeitlichen Gesichtspunkten nicht evaluierbar sind. Dies ist jedoch eine Voraussetzung für eine so genannte „sichere Ablaufplattform“.

Funktionsübersicht SDoT Diode®

Basisfunktionalität

- Unterstützt HTTP, SMTP, TCP, UDP
- Beschränkung auf zulässige Netzwerk- und Kommunikationsparameter
- Separierung durch Microkerneltechnologie
- Umfassende Protokollierung und Auditierung
- Alarmierung bei Sicherheitsverstößen und Störungen
- Fernadministration mittels Web-Schnittstelle
- Schutz vor Fehlbedienung und Fehlfunktionen, so dass ein Abfluss von Informationen aus HIGH auch im Fehlerfall nicht möglich ist
- Hochverfügbarkeitsvariante mit Failover (optional)

Datentransfer von LOW nach HIGH

- Hoch performante Datenübertragung
- **SDoT Diode®** fungiert als Proxy, Kommunikation wird zu beiden Netzen jeweils terminiert

Kein Datentransfer von HIGH nach LOW

- Unterdrückung sämtlicher Kommunikation von HIGH nach LOW
- Durch die Terminierung aller Verbindungen in der **SDoT Diode®** ist auch das Ausspähen von Betriebszuständen von Servern in HIGH aus LOW heraus nicht möglich

Zusammenfassung

Mit der **SDoT Diode®** stellt INFODAS GmbH eine sichere Datendiode für militärische und behördliche Anwendungen zur hoch-performanten Übertragung von Daten zwischen unterschiedlichen Sicherheitsdomänen zur Verfügung. Die **SDoT Diode®** liefert damit einen wichtigen Baustein für moderne IT-Infrastrukturen.

INFODAS - Gesellschaft für Systementwicklung und Informationsverarbeitung mbH
Rhonestr. 2
50765 Köln
Telefon (0221) 709 12 - 0
Fax (0221) 709 12 - 86
vertrieb@infodas.de
www.infodas.de