



# IT-Sicherheitslösungen für den öffentlichen Sektor

# Inhalt

<b>Vorwort</b>	<b>3</b>
<b>Zusammenfassung</b>	<b>4</b>
<b>Absicherung von Informations- und Kommunikationstechnologien im öffentlichen Sektor</b>	<b>5</b>
Shared-Services-Umgebungen	
“Grenzenlose” Netzwerke (Borderless Networks)	
Cisco und IT-Sicherheit	
<b>Sicherheit an der Netzwerkbasis</b>	<b>9</b>
Absicherung der Kontrollebene	
Absicherung der Datenebene	
Absicherung der Verwaltungsebene	
<b>Gefahrenabwehr am Perimeter</b>	<b>11</b>
Cisco Adaptive Security Appliance (ASA)	
Cisco Intrusion Prevention System (IPS)	
<b>E-Mail und Web-Sicherheit</b>	<b>13</b>
Cisco IronPort Email Security Appliances	
Cisco IronPort Web Security Appliances	
Cisco ScanSafe Cloud Web Security	
<b>Sichere Netzwerk-Overlays</b>	<b>16</b>
Dynamic Multipoint VPN (DMVPN)	
Group Encrypted Transport VPN (GET-VPN)	
Vergleich zwischen DMVPN- und GET-VPN-Implementierungen	
<b>Sichere Mobilität und Zugriffskontrolle</b>	<b>17</b>
Cisco TrustSec	
Cisco AnyConnect Secure Mobility Solution	
<b>Wie kann Cisco Sie unterstützen?</b>	<b>18</b>
<b>Weitere Informationen</b>	<b>19</b>

# Vorwort

Dieses Whitepaper enthält aktuelle und hilfreiche Informationen von Cisco zum Thema IT-Sicherheit für Einrichtungen der öffentlichen Hand.

Cisco hat zum Schutz vor Angriffen auf Informationsinfrastrukturen ein Konzept mit mehreren Säulen entwickelt. Dieses möchten wir unseren Partnern im öffentlichen Sektor mit diesem Whitepaper vorstellen.

Das vorliegende Dokument richtet sich an Entscheidungsträger im Sicherheitsbereich bei Behörden, im erweiterten öffentlichen Sektor sowie zugehörigen Unternehmen und Einrichtungen. Ziel ist es, das Sicherheitsbewusstsein aller Beteiligten zu schärfen. Dabei werden Wege aufgezeigt, wie IT-Sicherheitslösungen agiler, proaktiver und effizienter gestaltet werden können.

Angriffe auf Informationsinfrastrukturen sind heutzutage zunehmend komplexer und dynamischer. Dementsprechend ist es nicht nur entscheidend, überhaupt auf Bedrohungen vorbereitet zu sein, sondern auch in Sekundenschnelle dagegen vorgehen zu können. Dieses Dokument bietet Ihnen einen umfangreichen Ansatz, Ihre Einrichtung vor Bedrohungen zu schützen.

Entsprechende Technologien bilden die Grundlage für die Sicherheit eines Netzwerks und sind unabdingbar. Ein effizienter Schutz in vollem Maße baut jedoch auf weiteren Faktoren auf. So ist er nur gegeben, wenn die Mitarbeiter die Sicherheitsziele im Rahmen ihrer Prozesse und Arbeitsweise zu 100% unterstützen. Weitere Informationen zu wichtigen Aspekten in den Bereichen Personalwesen, Prozesse und Sicherheitsrichtlinien sind im Whitepaper „Cisco and Cyber Defence“ enthalten.

Gerne besprechen wir unser IT-Sicherheitskonzept persönlich mit Ihnen. Wir freuen uns darauf, Sie bei der Umsetzung Ihrer Ziele zu unterstützen.

**Cécile Willems**

Direktorin Vertrieb öffentliche Hand  
Cisco Deutschland

# Zusammenfassung

In den letzten Jahren wurde ein massiver Anstieg und die zunehmende Professionalisierung von Angriffen auf Informationsinfrastrukturen verzeichnet. Das Bundesministerium des Innern (BMI) stellt in seiner „Cyber-Sicherheitsstrategie für Deutschland“ die Bedeutung der Informations- und Kommunikationstechnik und damit die Bedrohung von IT-Angriffen für die gesellschaftlichen Grundlagen Deutschlands dar: „Staat, Kritische Infrastrukturen, Wirtschaft und Bevölkerung in Deutschland sind als Teil einer zunehmend vernetzten Welt auf das verlässliche Funktionieren der Informations- und Kommunikationstechnik sowie des Internets angewiesen. [...] Die Verfügbarkeit des Cyber-Raums und die Integrität, Authentizität und Vertraulichkeit der darin vorhandenen Daten sind zu einer existenziellen Frage des 21. Jahrhunderts geworden. Die Gewährleistung von Cyber-Sicherheit wird damit zur zentralen gemeinsamen Herausforderung für Staat, Wirtschaft und Gesellschaft im nationalen und internationalen Kontext.“

Diese kritischen Entwicklungen finden zu einer Zeit statt, in der viele Stellen der öffentlichen Hand ihre Strategie im Hinblick auf Informations- und Kommunikationstechnologien neu ausrichten. So werden Shared-Service-Umgebungen auf Basis gemeinsam genutzter IT-Infrastrukturen, -Anwendungen und -Dienstleistungen immer gängiger.

Da das Netzwerk den Kern dieser Umgebungen bildet, werden Sicherheitsaspekte immer wichtiger. So gilt es unter anderem, folgende Faktoren zu bedenken:

- Immer mehr Anwender greifen auf diese gemeinsam genutzten Infrastrukturen zu, das Sicherheitsrisiko steigt somit.
- Ihre Schlüsselkomponenten wie beispielsweise die Backbones der zugehörigen Netzwerke und Rechenzentren werden zu leicht identifizierbaren Angriffspunkten.
- In einer gemeinsam genutzten Infrastruktur werden zur Unterstützung der einzelnen Anwendergruppen oftmals Virtualisierungstechniken verwendet. Die Gewährleistung von Vertraulichkeit und Integrität der Daten jeder einzelnen Gruppe ist somit für eine wirksame Cyber-Sicherheit unerlässlich.

Angesichts dieser Umstände ist es dringend zu empfehlen, die Sicherheit der Infrastruktur eingehend zu analysieren und entsprechende Sicherheitsmaßnahmen zu implementieren. So sollte im Rahmen einer lokalen Strategievorgabe definiert werden, wie die bestehende Infrastruktur zur Schaffung einer Shared-Service-Umgebung angepasst und migriert werden kann. Es sollte klar erläutert werden, wie diese neuen Umgebungen zu schützen sind.

Das vorliegende Whitepaper beschreibt Empfehlungen von Cisco zum Schutz von modernen Netzwerk-Umgebungen. Dabei basiert das Konzept auf zwei Phasen.

- In der ersten Phase werden die **Möglichkeiten der Netzwerkbasis** ausgeschöpft. Mithilfe von integrierten Sicherheits- und Telemetriefunktionen wird das Netzwerk als Sicherheitssensor genutzt.
- In der zweiten Phase werden **vier Sicherheitslayer** implementiert, die für optimalen Schutz innerhalb des Netzwerks sowie am Perimeter sorgen.

Für die erste Phase eignet sich insbesondere das Programm „Turn it On“ von Cisco. Dabei kann mithilfe weniger Schritte sichergestellt werden, dass alle integrierten Sicherheitsfunktionen in der Netzwerk-basis aktiviert sind. Dies ist entscheidend für den weiteren Verlauf.

Sicherheitsbestimmungen sind nicht nur Teil der lokalen IT-Strategien von Organisationen. Sie müssen auch auf weiterreichende Ziele abgestimmt sein, welche auf Verlässlichkeit, Transparenz und Stabilität bauen. Grund hierfür sind die schwerwiegenden geschäftlichen Auswirkungen, die globale Reichweite sowie die rasante Ausbreitung von Angriffen auf IT-Infrastrukturen. Sie stellen daher eine ganz besondere Bedrohung dar. Bürger, Behörden und die Wirtschaft sind dabei die Hauptbetroffenen, die es bei der Entwicklung neuer Konzepte zur Abwehr von Angriffen zu unterstützen gilt.

Weitere Informationen zu diesem Thema sind im Whitepaper „Cisco and Cyber Defence“ enthalten. In diesem werden essenzielle Sicherheitsmaßnahmen besprochen, von denen wir erwarten, dass sie auf behördlicher Ebene in naher Zukunft obligatorisch sein werden. Sie erhalten einen klaren Leitfaden, wie Sie die Agilität und Reaktionsdynamik Ihres Netzwerks optimieren, die Sie zur Abwehr von sich stets wandelnden Angriffen benötigen.

Neben Technologien bietet Cisco auch Beratungs-Services für IT-Sicherheit an. So unterstützen wir bereits unterschiedliche Ministerien in folgender Form:

- Unterstützung bei der Entwicklung von Sicherheitsstrategien
- Durchführung von umfangreichen Sicherheitsanalysen der Infrastruktur
- Beratung hinsichtlich des Lebenszyklus von Technologien zur Verbesserung der Sicherheitsfunktionen und Identifizierung von Potenzialen zur Kostensenkung
- Entwicklung von Übergangsplänen zur Verbesserung der Sicherheitsfunktionen entsprechend geschäftlicher Anforderungen und neuen Lösungsmodellen
- Beratung zur optimalen Implementierung von Sicherheitstechnologien für die Netzwerkbasis und von Lösungen der vier Sicherheitslayer
- Unterstützung bei der Definition und Umsetzung der Information Assurance-Ziele

Gerne besprechen wir die Inhalte dieses Whitepapers persönlich mit Ihnen und erörtern, wie Cisco Sie im Bereich IT-Sicherheit unterstützen kann. Bitte wenden Sie sich als ersten Schritt an Ihren persönlichen Ansprechpartner bei Cisco.

# Absicherung von Informations- und Kommunikationstechnologien im öffentlichen Sektor

## Shared-Services-Umgebungen

In vielen Bereichen der öffentlichen Hand wurden bereits eigene lokale Strategien für Informations- und Kommunikationstechnologien eingeführt, die auf einer gemeinsamen Nutzung von Infrastruktur, Anwendungen und Services basieren. Sicherheitsaspekte sind in diesem Szenario aus verschiedenen Gründen von größter Bedeutung:

- Immer mehr Anwender greifen auf diese gemeinsam genutzten Infrastrukturen zu, das Sicherheitsrisiko steigt somit.
- Ihre Schlüsselkomponenten wie beispielsweise die Backbones der zugehörigen Netzwerke und Rechenzentren werden zu leicht identifizierbaren Angriffspunkten.
- In einer gemeinsam genutzten Infrastruktur werden zur Unterstützung der einzelnen Anwendergruppen oftmals Virtualisierungstechniken verwendet. Die Gewährleistung von Vertraulichkeit und Integrität der Daten jeder einzelnen Gruppe ist somit für eine wirksame IT-Sicherheit unerlässlich.

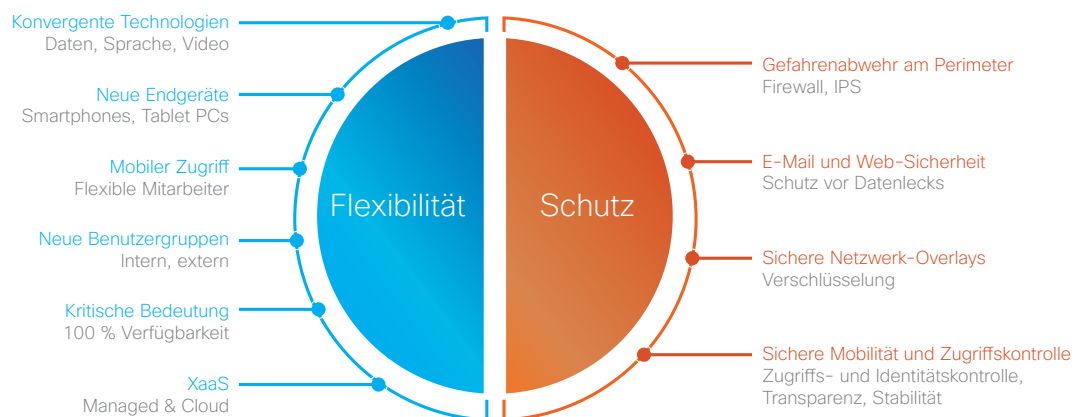
Wie wichtig der deutschen Regierung die Sicherheit von Shared-Services-Umgebungen ist, verdeutlichen die Inhalte der „Cyber-Sicherheitsstrategie für Deutschland“ sowie die Einrichtung des Nationalen Cyber-Abwehrzentrums.

## „Grenzenlose“ Netzwerke (Borderless Networks)

Das Konzept gemeinsam genutzter Infrastrukturen basiert auf intelligenten Netzwerken, die genügend Reichweite bieten, um Anwendergruppen innerhalb und außerhalb des öffentlichen Sektors zu unterstützen.

Cisco spricht hier von „Borderless Networks“ und verdeutlicht damit die Allgegenwärtigkeit von Netzwerktechnologien in der heutigen Zeit. Diese Netzwerke bieten eine unübertroffene Flexibilität (siehe Abbildung 1), birgen jedoch bei falschen Sicherheitsmaßnahmen auch ein erhöhtes Risiko für IT-Angriffe:

- Rasante technologische Veränderungen, erschweren die Identifikation und Nutzung von Best Practices
- Eine deutlich größere Reichweite kompliziert die Definition von Netzwerkgrenzen, sodass eine Vielzahl zusätzlicher Angriffspunkte entsteht
- Die stetig wachsende Anzahl an Anwendungen erfordert eine zunehmende Unterstützung und Absicherung für Daten-, Sprach- und Videoservices
- Die steigende Vielfalt an Endgeräten verlangt eine Unterstützung für verschiedenste Endgeräte wie auch private Smartphones und Tablet-PCs
- Neue Benutzergruppen wie beispielsweise mobile Mitarbeiter, Mitarbeiter von Subunternehmen, Geschäftspartner und Bürger benötigen unterschiedliche Zugriffsrechte
- Bereitgestellte Anwendungen über externe Verbindungen oder das Internet („as a Service“), müssen unterstützt werden.



Borderless Access – Flexibilität und Schutz



Der herkömmliche Ansatz zur Absicherung von Informations- und Kommunikationstechnologie sieht einen Schutz am Perimeter des Netzwerks vor. Damit sollen Bedrohungen vor allem externen Ursprungs vor dem Eindringen ins Netzwerk abgewehrt werden.

Dieser Ansatz stammt aus einer Zeit, in der Informations- und Kommunikationstechnologien anderweitig bereitgestellt wurden. Netzwerke hatten klar definierte Grenzen; die Unterstützung von Rechenzentren und Netzwerken war ausschließlich auf Datenservices beschränkt; Unternehmen hatten strenge Richtlinien im Hinblick auf Endgeräte und das Verhalten der Endbenutzer.

Heutzutage müssen sich Unternehmen jedoch gegen weitaus drastischere und aggressivere Netzwerkbedrohungen wehren. Komplexe Borderless Networks-Architekturen können nur mithilfe eines systematischen Sicherheitskonzepts auf Grundlage moderner, intelligenter Technologien geschützt werden, die auf mehreren Layern aufbauen und über selbst verteidigende Funktionalitäten verfügen.

Zur Absicherung von Borderless Networks-Architekturen hat Cisco ein Konzept entwickelt. Dieses gliedert sich in zwei klar voneinander abgegrenzte Phasen.

In der ersten Phase werden die Möglichkeiten der Netzwerkbasis ausgeschöpft. Mithilfe von integrierten Sicherheits- und Telemetriefunktionen wird das Netzwerk als Sensor genutzt. Hierbei kommen Funktionen zum Einsatz, die standardmäßig in allen Cisco-Produkten integriert sind. Sie unterstützen dabei, Bedrohungen auf der Netzwerk-Kontrollebene einzudämmen sowie das Verhalten auf der Netzwerk-Datenebene zu steuern und zu überwachen. Die letztgenannte Funktion ist besonders wichtig. Funktionen wie Cisco Netflow steuern dabei proaktive Reaktionen auf IT-Angriffe und sammeln detaillierte Informationen, um neu entstehende Bedrohungen identifizieren zu können.

In der zweiten Phase werden vier Sicherheitslayer (siehe Abbildung 2) implementiert, die entsprechend den Anforderungen für optimalen Schutz innerhalb des Netzwerks sowie am Perimeter sorgen:

- Gefahrenabwehr am Perimeter – um Bedrohungen einzudämmen, die durch unbefugten Zugriff an den Netzwerkgrenzen auftreten könnten. Typischerweise handelt es sich um externe Grenzen, aber auch interne Grenzen können betroffen sein, beispielsweise die eines Rechenzentrums.
- E-Mail und Web-Sicherheit – um Bedrohungen einzugrenzen, die bei der Übertragung von Inhalten über Websites oder E-Mails entstehen können. Dies ist insbesondere wichtig, um Datenlecks zu verhindern.
- Sichere Netzwerk-Overlays – zur Bereitstellung von Funktionen zur Netzwerkverschlüsselung. Somit kann die Vertraulichkeit und Integrität von Informationen während der Übertragung in Borderless Networks-Infrastrukturen gewährleistet werden.
- Sichere Mobilität und Zugriffskontrolle – zur Bereitstellung von Tools für effiziente Identitäts- und Zugriffskontrolle, sodass ein sicherer Netzwerkzugang für mobile Endgeräte und Mitarbeiter gewährleistet werden kann.

Weitere Informationen zu diesem Konzept von Cisco, unseren Sicherheitsfunktionen für die Netzwerkbasis sowie den vier Sicherheitslayern finden Sie auf den folgenden Seiten in den jeweiligen Abschnitten des Whitepapers.

## Cisco und IT-Sicherheit

IT-Sicherheit, oder auch Cyber-Sicherheit genannt, wird definiert als Schutz von Daten und Systemen in Netzwerken, die direkt oder durch elektronische Datenübertragung mit dem Internet verbunden sind.

Cyber-Attacken stellen eine akute Bedrohung für die Sicherheit von Behörden, Bürgern und Unternehmen dar. Zu ihren besonderen Merkmalen zählen ihre globale Reichweite sowie die rasante Ausbreitung.

Ein einziger Regierungsbereich allein kann die komplexen Herausforderungen im Zusammenhang mit IT-Attacken nicht bewältigen. Cisco kann als einer der führenden Anbieter von Netzwerktechnologien jedoch als starker Partner agieren, um bei der Entwicklung und Umsetzung einer Strategie gegen diese enorme Bedrohung zu unterstützen.

Cisco hat in diesem Zusammenhang bereits umfangreiche Verantwortung übernommen und unterstützt Unternehmen, Bürger wie auch Behörden dabei, Angriffe auf Informationsinfrastrukturen einzudämmen. Hierzu werden stets neue Ansätze und Technologien entwickelt wie beispielsweise die Cisco Security Intelligence Operations (SIO). Um Einblick in aktuelle sowie neu entstehende Bedrohungen zu gewinnen, werden dabei Informationen unserer weltweit installierten Produkte gesammelt und analysiert.

Cisco empfiehlt ein Konzept für IT-Sicherheit, welches auf drei Ideen basiert:

- **Verlässlichkeit** – Entwicklung eines Modells zur Identifizierung von Benutzern, Hosts, Netzwerkgeräten, Internet-Seiten, Mail-Servern etc., um die von ihnen gesendeten Informationen als vertrauenswürdig einzustufen.
- **Transparenz** – Verwendung des Netzwerks als Sensor, um mithilfe von Telemetrie-Tools seinen Zustand zu prüfen, unerwünschte Vorgänge zu erkennen und Netzwerkereignisse zu klassifizieren.
- **Widerstandsfähigkeit** – Entwicklung von Reaktionen, um Ausmaß und Auswirkungen eines Angriffs auf einzelne Prozesse sowie das Gesamtunternehmen zu minimieren.

In diesem Whitepaper werden einige der Funktionen erläutert, die Cisco nutzt, um die beschriebene Stabilität und Transparenz in IT-Infrastrukturen zu implementieren. Darüber hinaus wird Cisco in Kürze ein Begleitdokument mit dem Titel „Cisco and Cyber Defence“ veröffentlichen, das ausführlichere Informationen zum Thema Cyber-Sicherheit enthält.



„Ein einziger Regierungsbereich allein kann die komplexen Herausforderungen im Zusammenhang mit Cyber-Attacken nicht bewältigen. Cisco kann als einer der führenden Anbieter von Netzwerktechnologie jedoch als starker Partner agieren, um zu unterstützen.“

# Sicherheit an der Netzwerkbasis

Cisco hat sein Konzept für IT-Sicherheit ausgehend von der Netzwerkbasis entwickelt.

Über mehrere Jahre hat Cisco erhebliche Investitionen in die Einbettung von Sicherheitsfunktionen und -telemetrie in seine Standard-IOS-Betriebssystemsoftware getätigt. Diese sind in den wichtigsten Routing- und Switching-Lösungen integriert.

Diese standardmäßigen Sicherheitsfunktionen bieten den Benutzern bestmöglichen, sofort einsatzbereiten Schutz. Auf diese Weise wird die Sicherheit im Netzwerk optimiert und das bei lediglich geringen oder ganz ohne zusätzliche Kosten.

Um Kunden zu beraten, wie die integrierten Sicherheitsfunktionen genutzt werden können, um noch robustere, sicherere und stabilere Netzwerkinfrastrukturen zu schaffen, hat Cisco das Programm „*Turn it on*“ initiiert. Das Programm deckt verschiedene Cisco IOS-Softwarefunktionalitäten ab sowie spezifische Sicherheitsfunktionen und andere Tools zur Kontrolle der Datennutzung und Steuerung der Netzwerktopologie.

Cisco versteht das Netzwerk als aus drei Ebenen bestehend:

- Kontrollebene – wird von Protokollen verwendet, die das Netzwerk steuern wie beispielsweise Routing-Protokolle
- Datenebene – wird für die Weiterleitung von Datenverkehr verwendet
- Verwaltungsebene – wird zur Verwaltung und Überwachung der Netzwerkgeräte verwendet

Ein strukturierter Ansatz, zur Absicherung jeder dieser Ebenen ist für ein stabiles und leistungsfähiges Netzwerk unerlässlich. Auch Überprüfung und Überwachung müssen angemessen ausgeführt werden und können in Verbindung mit proaktiven Abwehrtechniken im Kampf gegen Cyber-Angriffe eine ausschlaggebende Rolle spielen.

## Sicherheit der Kontrollebene

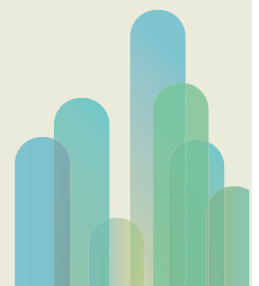
Die Kontrollebene eines Netzwerks umfasst zwei Elemente, die zwar getrennt voneinander betrachtet werden müssen, jedoch gewissermaßen auch miteinander verbunden sind. Das erste Element umfasst Protokolle einzelner Geräte, die eingesetzt werden, um lokale Ressourcen wie CPU und Speicher zu kontrollieren. Das zweite Element hingegen beschreibt die Protokolle, die innerhalb des Netzwerks eingesetzt werden, um Topologie und Stabilität zu kontrollieren. Die Elemente werden oft auch als Geräte- bzw. Netzwerk-Kontrollebenen bezeichnet.

Angriffe auf die Kontrollebene zielen meist auf einzelne oder mehrere Netzwerkgeräte ab und beeinträchtigen deren Fähigkeit, die internen Ressourcen zu kontrollieren oder ihre Rolle an der Netzwerk-Kontrolle wahrzunehmen. Bei derartigen Angriffen können auch fehlerhafte Kontrollinformationen eingespeist werden, um die Topologie zu destabilisieren und dadurch die Netzwerk- und Systemverfügbarkeit zu beeinträchtigen.

Cisco IOS Software bietet eine Reihe von Funktionen zum Aufbau einer sicheren Kontrollebene, wodurch Angriffe auf Geräte- und Netzwerk-Kontrollebenen minimiert werden. Drei Beispiele hierfür sind:

- **Device Control Plane Policing (CoPP)** – Einsatz von Richtlinien (z. B. Ablehnen, Durchsatzratenbeschränkung) für Netzwerkverkehr in Richtung der Kontrollebene eines Geräts. So wird eine Überlastung des Geräts und ein Denial of Service infolgedessen verhindert.
- **Routing Protocol Protection** – Authentifizierung von Routing-Peers und Routing-Updatequellen, um Netzwerk-Routingprotokolle robuster zu machen und dadurch die Layer 3-Topologie zu schützen.
- **Spanning Tree Toolkit** – Funktionen in den Cisco Catalyst Switches zur Kontrolle und Verwaltung von Spanning Tree-Meldungen, wodurch die Layer 2-Topologie geschützt wird.

„Mit dem Programm *Turn it On* können integrierte Sicherheitsfunktionen optimal genutzt und so robustere, sicherere und stabilere Netzwerkstrukturen geschaffen werden.“



## Sicherheit der Datenebene

Die Datenebene eines Netzwerks umfasst die Pfade, über die der Datenverkehr im Netzwerk stattfindet. Dazu zählen sowohl die Pfade innerhalb der einzelnen Netzwerkgeräte als auch die zwischen verschiedenen Netzwerkgeräten.

Angriffe auf die Datenebene zielen auf einzelne oder mehrere Netzwerkgeräte ab und überfluten diese mit fehlerhaftem Datenverkehr. Folglich kann der Netzwerkservice nicht aufrechterhalten werden. Diese Attacken werden als „Denial-of-Service-Angriffe“ bezeichnet.

Bei fehlerhaftem Datentransfer kann es sich um falsch strukturierte, falsch adressierte oder fehlgeleitete Datenpakete handeln. Die Cisco IOS Software bietet eine Reihe von Funktionen zum Schutz der Datenebene durch Identifizierung und Eindämmung von derartigen Angriffen. Beispiele solcher Funktionen sind:

- **Unicast Reverse Path Forwarding (uRPF)** – blockiert IP-Verkehr mit einer gefälschten (gespoofen) Quell-IP-Adresse. Dazu werden eingehende Pakete mit der Routing-Tabelle des Gerätes verglichen, um sicherzustellen, dass sie an der richtigen Schnittstelle ankommen.
- **Zugangskontrolllisten** – bieten Funktionen (Zulassen, Ablehnen etc.), um die Weiterleitungsfunktionen der Netzwerkgeräte zu limitieren. So wird die Kapazität des Netzwerkzugangs eines Angreifers eingeschränkt.

„Netzwerk-Telemetrie spielt besonders bei der Eindämmung von Cyber-Angriffen eine wichtige Rolle. Mithilfe der dadurch entstehenden Transparenz wird das Netzwerk zu einem Sensor, mit dem sein Zustand überwacht, unerwünschte Vorgänge identifiziert und Netzwerkereignisse klassifiziert werden können.“

## Sicherheit der Verwaltungsebene

Die Verwaltungsebene eines Netzwerks dient zur Kontrolle und Verwaltung von physischen Netzwerkgeräten.

Angriffe auf die Verwaltungsebene zielen auf einzelne oder mehrere Netzwerkgeräte ab, sodass ein Angreifer die Funktion, Leistung oder Verfügbarkeit eines Netzwerks ändern und damit den Benutzern schaden kann.

Jegliche Beeinträchtigung der Verwaltungsebene kann einem Angreifer ausgezeichnete Kontrollmöglichkeiten über die Netzwerkinfrastruktur verschaffen. Die Cisco IOS Software bietet eine Vielzahl von Funktionen zum Schutz der Verwaltungsebene und zur Eindämmung derartiger Angriffe. Beispiele solcher Funktionen sind:

- **Secure Remote Access** – dank verschlüsselten Remote Access-Protokollen wie SSH und HTTPS sowie Zugangskontrolllisten, die nur vertrauenswürdigen IP-Adressen Zugriff gestatten, wird der Umfang eines Angriffes eingeschränkt.
- **Rollenbasierter Zugang** – das Prinzip der geringstmöglichen Privilegien ist entscheidend in der Informationssicherheit. So wird sichergestellt, dass Administratoren Zugriffsrechte besitzen, die ihren Rollen entsprechen. Sowohl böswillige als auch unbeabsichtigte Beschädigungen werden begrenzt.
- **Netzwerktelemetrie** – Sicherheitsüberwachung ist eines der wirkungsvollsten Tools zur Eindämmung aktueller und neu entstehender Sicherheitsbedrohungen. Cisco Netflow bietet Administratoren einen detaillierten und umfassenden Einblick in den Datenverkehr eines Netzwerks. So lassen sich in Verbindung mit entsprechenden Analysetools ungewöhnliche Aktivitäten schnell identifizieren und offensichtliche Vorfälle wie Denial-of-Service-Angriffe klassifizieren.

Netzwerk-Telemetrie spielt besonders bei der Eindämmung von Cyber-Angriffen eine wichtige Rolle. Mithilfe der dadurch entstehenden Transparenz wird das Netzwerk zu einem Sensor, mit dem sein Zustand überwacht, unerwünschte Vorgänge identifiziert und Netzwerkereignisse klassifiziert werden können.

Zudem gibt es noch weitere Funktionen von IOS-Geräten, die die oben genannten Sicherheitsfunktionen ergänzen. So können Geräte von Cisco vielfältige und komplexe Quality of Service-Richtlinien unterstützen. Diese stellen beispielsweise sicher, dass die Netzwerkverfügbarkeit für Echtzeit-Protokolle nicht beeinträchtigt werden kann – auch nicht durch extrem hohe Datenverkehrslasten.

# Gefahrenabwehr am Perimeter

Früher wurden IT-Infrastrukturen auf Grundlage von klar definierten Kabelnetzwerken mit entsprechenden Domain-Parametern entwickelt. Es wurde angenommen, dass Netzwerkangriffe ihren Ursprung stets außerhalb des Unternehmens haben. Daher basierten die Abwehrmechanismen auf der Erstellung von gut geschützten Netzwerk-Perimetern.

Durch das Aufkommen von Borderless Networks-Architekturen ist es viel schwieriger geworden, diese Parameter zu definieren und zu schützen. Grund hierfür sind die unterschiedlichen Gateway-Verbindungen sowie die Reichweite von Wireless- und VPN-Technologien heutzutage.

Folglich bleibt der Aufbau einer sicheren Netzwerkbasis oberste Priorität, während gleichzeitig jedoch auch eine robuste Gefahrenabwehr am Perimeter des Netzwerks implementiert werden muss zum Schutz der Ein- und Ausgangspunkte. Die Gefahrenabwehr am Perimeter stellt den ersten der vier Sicherheitslayer dar.

Gängige Technologien zum Schutz am Netzwerk-Perimeter wie Firewalls und Intrusion Prevention Systeme (IPS) sind schon seit geraumer Zeit erhältlich. Die meisten modernen Geräte verfügen allerdings über zahlreiche neue Funktionen, eine höhere Leistungsfähigkeit und sind virtualisiert, um den Nutzen und die Wiederverwendbarkeit ihrer Funktionen zu maximieren.

Cisco bietet zwei Produktgruppen zur Gefahrenabwehr am Perimeter:

- Cisco Adaptive Security Appliance (ASA) mit Firewalling der Enterprise-Klasse
- Network IPS Appliances zur Überprüfung und Überwachung des Datenverkehrs

Die ASA- und IPS-Geräte sollten an allen physischen oder logischen Domain-Grenzen eines Netzwerks implementiert werden. Normalerweise handelt es sich um externe Grenzen – zum Beispiel an Gateways zu Backbone-Netzwerken. Aber auch interne Grenzen kommen in Frage – zum Beispiel am Eingangspunkt eines Rechenzentrums oder zwischen Funktionslayern innerhalb eines Rechenzentrums.

## Cisco Adaptive Security Appliance (ASA)

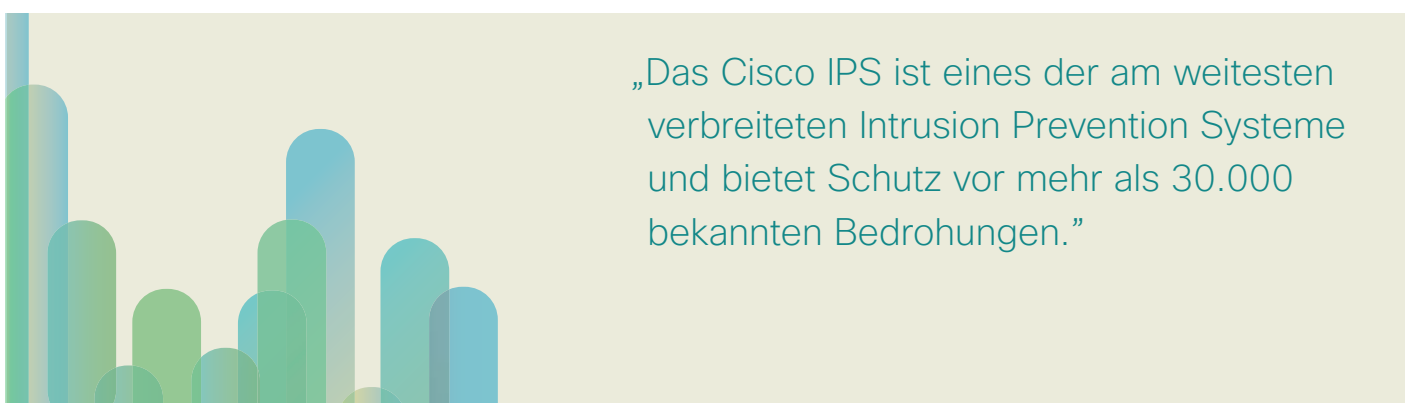
Cisco ASA ist eine Sicherheitslösung der Enterprise-Klasse, die eine führende Firewall und Remote-Zugriffsfunktionen über VPN mit Intrusion Prevention und optionalen Content Security-Funktionen verbindet.

Die Cisco ASA Firewall lässt den regulären Datenverkehr im Unternehmen unbeeinträchtigt, während unerwünschter Verkehr basierend auf verschiedenen Steuerungsfunktionen für Anwendungen geblockt wird. Durch diese Steuerungsfunktionen werden die internen Sicherheitsrichtlinien implementiert, um Peer-to-Peer-Filesharing, Instant Messaging und schadhafte Datenverkehr entsprechend zu begrenzen. Die sichere Implementierung von neuen Geschäftsanwendungen wird jedoch nicht beeinträchtigt.

Cisco ASA Remote VPN bietet Site-to-Site und Remote-VPN-Zugriff auf interne Netzwerksysteme und -services. SSL und IPsec VPN-Optionen sorgen für ein hohes Maß an Flexibilität. Durch die Kombination von Firewall- und Content-Security Services mit Remote Zugriff mittels VPN-Services bietet Cisco ASA eine besonders robuste Lösung, die Risiken von Malware sowie das Bedrohungspotenzial durch Remote-VPN-Geräte minimiert.

Cisco ASA verfügt über Erweiterungssteckplätze zur Unterstützung neuer Zusatzfunktionen. Die Lösung ist sofort einsatzbereit und kann für Firewall, Remote-VPN-Zugang und andere Funktionen genutzt werden, um mit den sich ändernden Geschäftsanforderungen und Sicherheitsbedrohungen Schritt zu halten.

Sie bietet auch Intrusion Prevention-Funktionen, die als Einzellösung betrieben oder für die Verbindung mit Cisco SensorBase – ein Teil der Security Intelligence Operations (SIO) von Cisco – konfiguriert werden können. Über die Verbindung mit Cisco SensorBase wird stündlich die neueste Liste bekannter Botnet-Befehle und Control-Hosts über die Cisco Datenbank abgerufen, die dann abgeblockt werden können.



## Cisco Intrusion Prevention System (IPS)

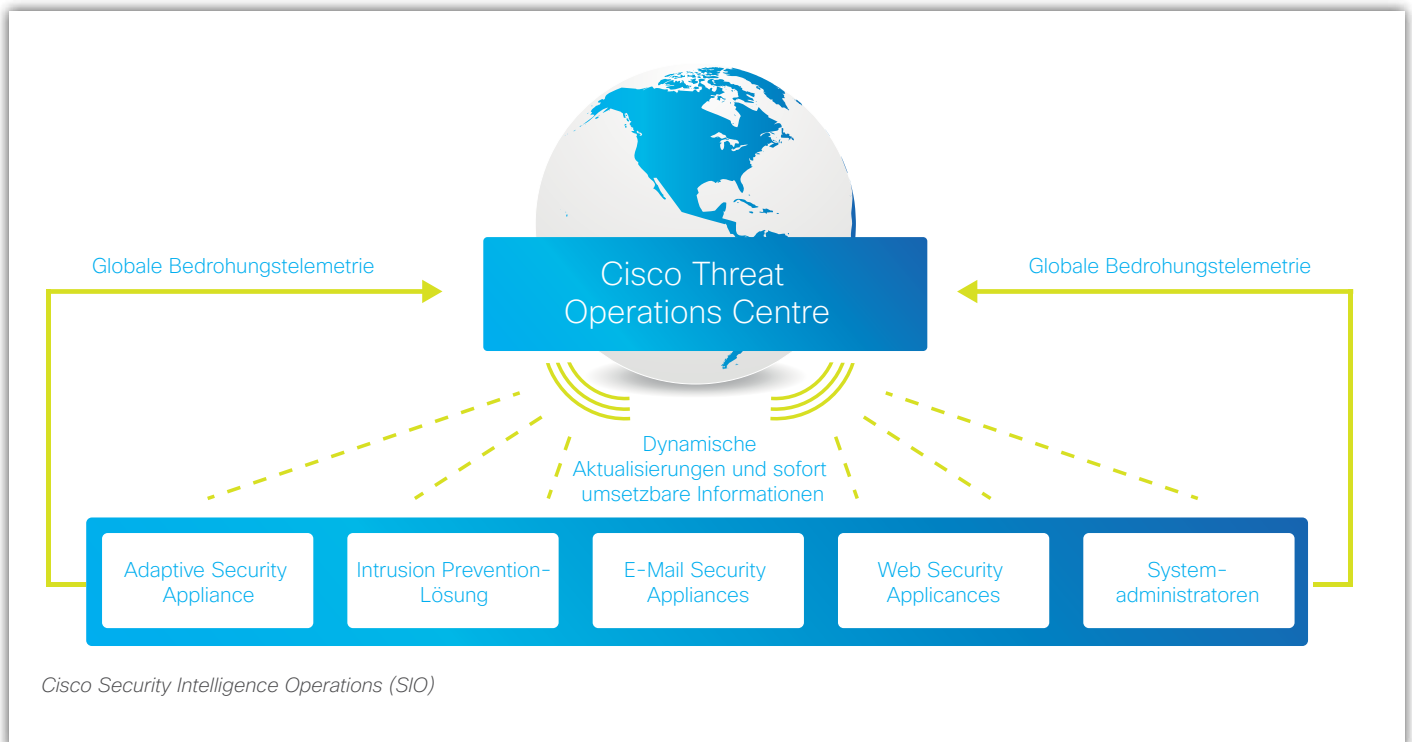
Cisco IPS sollte zusammen mit einer Firewall implementiert werden, um physische und logische Domain-Grenzen am Perimeter und innerhalb eines Netzwerks zu schützen.

Da Cisco IPS bekannte wie unbekannte Sicherheitsbedrohungen an jeglichen Grenzen des Netzwerks identifizieren, klassifizieren und beseitigen kann, spielt es für die erfolgreiche Implementierung von Borderless Networks-Architekturen eine entscheidende Rolle. Cisco IPS ist eine der Schlüsselkomponenten, die das Netzwerk zu einem Sensor macht und für Transparenz sorgt, um Cyber-Attacks einzudämmen.

Cisco IPS ist eines der am weitesten verbreiteten Intrusion Prevention Systeme und bietet Schutz vor mehr als 30.000 bekannte Bedrohungen. Es bietet Schutz vor zunehmend ausgeklügelten Angriffen wie beispielsweise gezielte Attacks, Würmern, Botnets, Malware und Anwendungsmissbrauch. Regelmäßige Signatur-Updates in Kombination mit der Cisco Global Correlation-Funktion innerhalb jedes IPS ermöglichen die dynamische Erkennung, Bewertung und Beseitigung von aktuellen und neu entstehenden Bedrohungen aus dem Internet.

Ähnlich Cisco ASA kann auch Cisco IPS so konfiguriert werden, dass eine Verbindung mit Cisco Security Intelligence Operations (SIO) hergestellt wird. Auf diese Weise können jederzeit aktuelle Reputationsinformationen über den Host in Echtzeit abgefragt werden. Diese einzigartigen Kontextinformationen werden von der Cisco Global Correlation Funktion der IPS verwertet und fließen schließlich in die dynamische Bedrohungsanalyse ein, um die Wahrscheinlichkeit von böswilligen Absichten in Verbindung mit Netzwerkereignissen zu ermitteln.

Wichtig ist dies in Fällen, in denen Cisco IPS einen Vorgang erkennt, der zwar oft auftritt, aber nicht immer mit schädlichen Aktivitäten verbunden ist. Ohne Global Correlation würde IPS den Vorfall melden, jedoch würden keine Maßnahmen bezüglich des Netzwerkverkehrs ergriffen werden. Mit der Global Correlation-Funktion hingegen hat der Sensor die Möglichkeit, Informationen über die Reputation der Datenverkehrsquelle abzurufen. Bei schlechter Reputation kann der Sensor direkt reagieren und den potenziellen Angriff abwehren, ohne dabei den regulären Datenverkehr zu beeinträchtigen. Reputationsdaten können von Cisco IPS auch anderweitig verwendet werden. So beispielsweise kann der Datenverkehr von Quellen mit sehr schlechter Reputation vorbeugend gefiltert werden, um Rechenleistung für anderen Verkehr freizuhalten.



# E-Mail und Web-Sicherheit

In den letzten Jahren ist die Anzahl neuer Bedrohungen, Störungen und Risiken immer weiter angestiegen. Öffentliche Einrichtungen müssen mit entsprechenden Sicherheitsrichtlinien und -strategien für diese Risiken gewappnet sein.

Zwei Angriffsmittel erfordern besondere Aufmerksamkeit:

- E-Mails sind zu einem beliebten Mittel geworden, um Geräte zu infizieren oder per Phishing an vertrauliche Daten zu gelangen.
- Web-Inhalte haben sich zum meistgenutzten Medium zur Infizierung von Endgeräten entwickelt, wobei der Benutzer davon oft nichts bemerkt.

E-Mail-Verkehr und Web-Inhalte eignen sich nicht nur für derartige Angriffe, sondern bieten auch Zugriffsmöglichkeiten auf vertrauliche Informationen. Organisationen der öffentlichen Hand müssen sich bewusst sein, dass diese Kanäle eine reale Gefahr darstellen, die zum Datenverlust führen kann, sei es durch böswillige Absichten oder durch unbeabsichtigte Vorfälle.

Der Schutz von E-Mail- und Web-Inhalten wird unter dem zweiten Sicherheitslayer im Konzept von Cisco zusammengefasst. Dabei werden die oben genannten Bedrohungen und Störungen adressiert und ein umfassender Schutz des Netzwerkperimeters in Ergänzung zu Cisco ASA und Cisco IPS bereitgestellt.

## Cisco IronPort Email Security Appliances

Cisco IronPort Email Security Appliances bieten eine Vielzahl von Sicherheitsfunktionen zur Kontrolle von ein- und ausgehenden E-Mails. Mit den Appliances profitieren Organisationen im öffentlichen Sektor von zwei wesentlichen Vorteilen:

- Überwachung und Kontrolle von eingehenden E-Mails zum Schutz vor Cyber-Attacken und Spam
- Überwachung und Kontrolle von ausgehenden E-Mails zum Schutz vor Datenverlust

Früher wurden eingehende E-Mails durch signaturbasierte Softwarelösungen überwacht und kontrolliert, die in den Kopfzeilen oder im Text der E-Mails nach bestimmten Wörtern oder Wortkombinationen suchten. Mit gesteigertem E-Mail-Aufkommen und komplexeren Spammessages waren jedoch neue Lösungen vonnöten, nicht zuletzt, um auch die Kosten für die Verarbeitung zu reduzieren. Cisco hat eine neue Technik entwickelt, die als „Reputation Filtering“ bezeichnet wird.

Durch Reputation Filtering wird jeder sendenden E-Mail-Domain eine Reputationbewertung zugewiesen. Auf Grundlage der Reputation der Absender-Domain-Adresse können die Appliances entscheiden, ob eine E-Mail vertrauenswürdig ist oder eventuell eine Sicherheitsbedrohung darstellt beziehungsweise als Spam eingestuft werden sollte. Je höher die Reputation einer Domäne, desto geringer die Wahrscheinlichkeit, dass eine Nachricht ein Risiko darstellt oder es sich um Spam handelt.

Cisco IronPort Email Security Appliances erhalten Informationen über die Reputation des Senders von eingehenden E-Mails in Echtzeit. Hierzu werden Datensätze der Cisco SensorBase abgefragt. SensorBase ist eine Komponente der Security Intelligence Operations (SIO) von Cisco. Hier werden unter anderem auch Informationen zur Bewertung der Reputation von IP-Adressen gesammelt und analysiert, welche dann Cisco IronPort Email Security Appliances zur Verfügung gestellt werden.

Die Reputationbewertungen basieren auf der Erfassung, Aggregation und Gewichtung von mehr als zweihundert verschiedenen E-Mail-Parametern. Dabei ergibt sich letztendlich ein Reputationswert zwischen -10,0 für den vertrauensunwürdigsten und +10,0 für den vertrauenswürdigsten E-Mail-Server. E-Mails von Servern mit schlechter Bewertung (in der Regel unter -3,0) werden von den Appliances zurückgewiesen. Für Sender mit mittlerer bis schlechter Bewertung können Durchsatzratenbeschränkungen festgelegt werden. Zudem besteht die Möglichkeit, eine „White List“ für E-Mail-Server von Fortune 1.000-Unternehmen mit guten Bewertungen von 9,0 und höher zu erstellen.

Cisco IronPort Email Security Appliances können schädliche E-Mails äußerst zuverlässig erkennen. So berichten die meisten unserer Kunden, dass durch Standardeinstellungen der Appliances mehr als 90% der eingehenden Spammessages geblockt werden. Diese erste Verteidigungslinie reduziert das Gesamtvolumen an eingehenden E-Mails, sodass andere nachgeschaltete Viren- und Spamscanner mittels Deep Packet Inspection weitere Prüfungen der E-Mails vornehmen können.

## Schutz vor Datenverlust

Die Verhinderung von Datenverlusten ist für die öffentliche Hand zum Schutz der vertraulichen Informationen von Bürgern und Unternehmen von größter Bedeutung. Dies ist besonders kritisch, da Behörden immer weniger zentralisiert und ihre Standorte und Mitarbeiter weiter verteilt sind. Damit wird die Überwachung der Aktivitäten Einzelner immer schwieriger.

Cisco Data Loss Prevention (DLP) bietet Schutz vor Datenlecks und hilft, Risiken besser zu bewerten und Datenverlust zu verhindern. Dabei werden vertrauliche Informationen durch die Implementierung von Richtlinien im Hinblick auf Inhalt, Kontext und Ziel des Datenverkehrs im Internet oder in E-Mails geschützt.

Cisco DLP ist als Erweiterung von Cisco IronPort Email Security Appliances erhältlich. Es wird in Verbindung mit Technologien von RSA implementiert und als Software für die Appliances geliefert.

## E-Mail-Verschlüsselung

E-Mails sind zu einer der gängigsten Kommunikationsmöglichkeiten geworden. Daten können in unterschiedlichsten Umgebungen schnell und einfach weitergeleitet werden. Dies führt aber auch zu entsprechenden Missbrauchsmöglichkeiten.

Vor allem angesichts der Tatsache, dass E-Mails teils auch zur Bearbeitung von vertraulichen Bürger- und Patientendaten verwendet werden. Hierbei besteht eine reale Gefahr, dass diese Daten nicht in Übereinstimmung mit internen Sicherheitsrichtlinien einer Einrichtung oder sogar mit den gesetzlichen Vorschriften geschützt sind.

Zur Verschlüsselung von E-Mails verwendet Cisco eine Methode, die als „Secure Envelopes“ bezeichnet wird. Sie ist einfach zu nutzen und ermöglicht die schnelle und sichere Übertragung vertraulicher Daten. Auch der Austausch verschlüsselter E-Mails mit Dritten ist möglich.

Der Absender muss sich nicht um die Verschlüsselung von E-Mails kümmern, da die zentrale E-Mail Security Appliance diese Aufgabe übernimmt. Dies geschieht basierend auf vordefinierten Regeln zur Verschlüsselung von Nachrichten, die je nach Absender, Empfänger oder Inhalt der Nachricht angelegt werden können. Ein E-Mail-Empfänger muss den Absender nicht kennen, um die Nachricht zu entschlüsseln.

So können Mitarbeiter im öffentlichen Dienst sicherstellen, dass vertrauliche Daten in E-Mails geschützt bleiben, auch wenn sie an Außenstehende gesendet werden.

## Cisco IronPort Web Security Appliances

Früher wurden Sicherheitsfunktionen für Web-Inhalte implementiert, um den Zugriff auf bedenkliche Inhalte zu blocken und Produktivitätsseinbußen durch arbeitsfremde Anwendungen zu verhindern. Zusätzlich sind heutzutage jedoch auch Technologien zur Absicherung der Internetnutzung gefragt, um Bedrohungen durch Phishing-Inhalte und Websites einzudämmen, die durch Manipulation schädliche Inhalte verbreiten.

In der Vergangenheit waren Technologien zur Absicherung des Internets auf statisches Filtern ausgerichtet, um schädliche oder bedenkliche Web-Inhalte zu identifizieren. Mechanismen zur Reputationsbewertung für Web-Domains – ähnlich wie sie für E-Mail-Domainnamen verwendet werden – haben die Techniken mittlerweile erheblich verbessert.

Cisco IronPort Web Security Appliances führen eine dynamische Kalkulation des Risikos für jede Internetanfrage und -antwort durch. Zusammen mit signatur- und verhaltensbasierten Scans bieten Web-Reputationsfilter viel schnellere und effektivere Internet-Sicherheitsfunktionen mit mehreren Layern. Reputationsinformationen werden verwendet, um Transaktionen mit hohem Risiko zu blocken und Benutzer vor Angriffen wie IFrame und Cross Site Scripting zu schützen.

Cisco IronPort Web Security Appliances rufen im Abstand von fünf Minuten aktualisierte Reputationsinformationen über die Cisco SIO SensorBase-Datenbank ab. Diese Regelpakete enthalten Listen problematischer Web-Hosts sowie Informationen über infizierte URLs und Internet-Seiten. Durch schnelle, präzise Scans aller Objekte auf einer Webseite ist die Erkennung infizierter Inhalte weitaus wahrscheinlicher als bei Methoden, die lediglich die URL selbst oder die erste HTML-Abfrage prüfen.

## Cisco ScanSafe Cloud Web Security

Die Schere zwischen dem Bedarf an Diensten der öffentlichen Hand und dem zur Verfügung stehenden Budget geht weiter auseinander. Es sind also grundlegende wirtschaftliche Änderungen vonnöten, um dieser Problematik begegnen zu können.


Beispielsweise die Nutzung cloud-basierter Services für Informations- und Kommunikationstechnologien. So können neue nutzungsorientierte Modelle gefördert und Kosten reduziert werden.

Hier greift die Cisco ScanSafe Web Security-Lösung, ein cloud-basierter Sicherheits-Service, der verhindern soll, dass Zero-Day-Malware-Attacken die Borderless Networks-Architekturen von Behörden erreichen können. Dabei wird weder eine neue Hardware benötigt, noch fallen Wartungskosten oder ähnliches an. Die Lösung bietet einzigartigen Schutz gegen Echtzeit-Bedrohungen sowie höchste Zuverlässigkeit mit 100% Verfügbarkeit seit mehr als acht Jahren. Damit ist jederzeit ein sicherer Zugriff auf das Internet gewährleistet.

Mit Cisco ScanSafe Web Security-Lösungen können präzise Richtlinien für jeglichen Internet-Datenverkehr inklusive SSL-verschlüsselter Kommunikation erstellt werden. Sicherheitsrichtlinien lassen sich auf Grundlage von Kategorien, Inhalten, Dateitypen und Kontingenten erstellen und genau anpassen. In Kombination mit einer integrierten Outbound-Richtlinienfunktion wird somit sichergestellt, dass vertrauliche Inhalte wie Kundendaten oder Kreditkartennummern das Netzwerk nicht verlassen.

Basierend auf definierten Sicherheitsrichtlinien analysiert die Lösung außerdem sämtliche Internetanfragen, um festzustellen, ob Inhalte bösartig, bedenklich oder akzeptabel sind. Dies ermöglicht einen effektiven Schutz, auch gegen Zero-Day-Bedrohungen, die ansonsten erheblichen Schaden verursachen würden.

Zusammen mit dem Cisco AnyConnect 3.0 Client bietet die Cisco ScanSafe-Lösung jetzt eine konsistente Richtliniendurchsetzung für die Web-Sicherheit – nicht nur für Büroräume, sondern auch für standortferne und mobile Mitarbeiter. Durch Cisco AnyConnect wird sämtlicher Internet-Datenverkehr über das nächste ScanSafe-Rechenzentrum transparent weitergeleitet. So wird sichergestellt, dass Geräte geschützt sind, auch wenn die Verbindung zum Netzwerk getrennt ist.



„DMVPN verbindet drei separate Internet-Standardprotokolle – IPsec, Next Hop Resolution Protocol (NHRP) und Generic Route Encapsulation (GRE). So können ein einfacher Hub-and-Spoke-Tunnel-Overlay erstellt und automatisch dynamische On-Demand-Spoke-to-Spoke-Tunnel eingerichtet werden.“

# Sichere Netzwerk-Overlays

Die Wahrung der Informationsvertraulichkeit innerhalb eines Wide Area Network (WAN) spielt für alle Behörden eine enorme Rolle; vor allem, wenn sie Vertraulichkeitsklassifizierungen verwenden oder vertrauliche Bürger- oder Patientendaten bearbeiten.

Bereits seit vielen Jahren unterstützt und entwickelt Cisco Tools zur Verschlüsselung auch umfassender Wide Area Networks. Basierend auf IP Security (IPsec)-Standards hat Cisco konstant neue Innovationen in Form skalierbarer Schutzmechanismen mit geringen Verwaltungskosten geschaffen.

Die Verschlüsselungsoptionen für sichere Netzwerk-Overlays bilden den dritten der vier Layer im Konzept von Cisco.

## Dynamic Multipoint VPN (DMVPN)

Mit der Einführung von Dynamic Multipoint VPN (DMVPN) vor einigen Jahren wurde auf die Skalierungseinschränkungen von Kunden reagiert, die sowohl Hub-to-Spoke-Kommunikation (für den Zugriff auf zentrale Rechenzentren) als auch direkte Spoke-to-Spoke-Kommunikation (für Echtzeitanwendungen wie IP-Voice und -Video) benötigen.

DMVPN verbindet drei separate Internet-Standardprotokolle – IPsec, Next Hop Resolution Protocol (NHRP) und Generic Route Encapsulation (GRE). Es ist somit möglich, einen einfachen Hub-and-Spoke-Tunnel-Overlay zu erstellen und automatisch dynamische On-Demand-Spoke-to-Spoke-Tunnel einzurichten.

Vor der Entwicklung von DMVPN mussten IPsec-Tunnelnetze manuell erstellt werden, zumindest teilweise und in nicht wenigen Fällen sogar vollständig. Dies führte zu komplexen Gerätekonfigurationen und hohen Verwaltungskosten.

## Group Encrypted Transport VPN (GET-VPN)

Der zweite und neuere Ansatz von Cisco für verschlüsselte Overlays ist Group Encrypted Transport VPN (GET-VPN).

GET-VPN wurde speziell für die Implementierung in privaten MPLS WANs konzipiert (DMVPN kann in einem privaten WAN oder im Internet implementiert werden) und bietet tunnelfreie Verschlüsselung.

Um dies zu erreichen, hat Cisco den neuen Standard Group Domain of Interpretation (GDOI) weiter verbessert, um ein Overlay-Group-Encryption-Modell zu entwickeln. Dadurch kann jedes Gerät, das der Gruppe beitreten darf, mit jedem anderen Gerät in der Gruppe kommunizieren, ohne dass dabei Tunnel erstellt oder definiert werden müssen.

Mit diesem Verschlüsselungsansatz kommt ein Konzept zum Einsatz, bei dem in jeder IPsec-Domäne ein Schlüsselserver eingesetzt wird. Der Schlüsselserver verwaltet für alle Gruppenmitglieder einen gemeinsamen Kodierungsschlüssel, der regelmäßig geändert wird, und dient als zentrale Stelle der Richtlinienkontrolle. Daher ist es nicht mehr nötig, die Verschlüsselungsrichtlinie für neue Gruppenmitglieder explizit zu definieren.

## Vergleich zwischen DMVPN- und GET-VPN-Implementierungen

DMVPN und GET-VPN verwenden ähnliche Ansätze, um allgemeine Geschäfts- und Sicherheitsherausforderungen zu bewältigen, mit denen die Regierung und der öffentliche Sektor konfrontiert sind.

Der Hauptunterschied besteht in der Art des Sicherheitsmodells. Das Sicherheits- und Zugriffskontrollmodell des DMVPN ist identisch mit herkömmlichen Point-to-Point IPsec-Implementierungen: Es teilen sich also je zwei Verschlüsselungsendgeräte einen gemeinsamen Kodierungsschlüssel und tauschen Informationen paarweise untereinander aus. Wie oben beschrieben ist beim GET-VPN der Schlüsselserver für die Zugriffskontrolle und die Verwaltung eines gemeinsamen Kodierungsschlüssels für alle Geräte in der Gruppe verantwortlich. Mitglieder können der Gruppe gegen Vorlage eines gültigen Zertifikats, üblicherweise in digitaler Form, beitreten, das von einer Public Key Infrastructure (PKI) vergeben wird. Informationen werden dann gruppenweise ausgetauscht.

DMVPN und GET-VPN nutzen unterschiedliche Modelle der Zugriffskontrolle, sind jedoch beide äußerst skalierbar und unterstützen bis über 10.000 Geräte. Im Vergleich zu herkömmlichen Hub-and-Spoke-Lösungen sind die Verwaltungskosten relativ gering.

Cisco bietet beide dieser Overlay-Optionen für Netzwerksicherheit. Sowohl DMVPN als auch GET-VPN sind erhältlich als optionale lizenzierte IOS-Software für WAN CPE-Router, wie zum Beispiel den Cisco ISR G2.

Vergleichende Informationen zu den VPN-Technologien von Cisco erhalten Sie hier:

[http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6635/ps7180/prod\\_brochure0900aecd80582078.pdf](http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6635/ps7180/prod_brochure0900aecd80582078.pdf)

# Sichere Mobilität und Zugriffskontrolle

Traditionelle Kabelnetzwerke werden zunehmend ersetzt durch Borderless Networks-Architekturen, eine Kombination aus Kabel- und Wireless-Netzwerken sowie VPNs.

Dies erschwert es jedoch auch, die Perimeter des Netzwerks zu definieren. Genau dort muss aber für Sicherheit gesorgt werden, denn sie stellen gleichzeitig auch die Zugangspunkte für mobile Mitarbeiter dar, welche auf Anwendungen und Services zugreifen.

Dynamische, standortunabhängige Mitarbeiter stellen für Organisationen des öffentlichen Sektors einen enormen wirtschaftlichen Vorteil dar. Gleichzeitig ergeben sich dadurch jedoch auch erhebliche Herausforderungen für IT-Abteilungen, sowohl hinsichtlich der Service-Bereitstellung als auch mit Blick auf die Gewährleistung der Sicherheit.

Cisco hat mehrere Lösungen zur sicheren Mobilität und Zugriffskontrolle entwickelt, um diesen Herausforderungen zu begegnen. Sie bilden den vierten Sicherheitslayer des Konzepts von Cisco. Hierzu gehören unter anderem folgende Produkte:

- Cisco TrustSec – für identitätsbasierten Zugriff auf gemeinsam genutzte Netzwerke
- Cisco AnyConnect – für sicheren, richtlinienbasierten Zugriff mobiler Endgeräte auf gemeinsam genutzte Netzwerke

## Cisco TrustSec

Cisco TrustSec ist eine von mehreren Funktionen, die in Lösungen der Cisco Borderless Networks-Architektur integriert sind.

Mit ihr können mobile Mitarbeiter bestens unterstützt werden bei gleichzeitigem Schutz der Netzwerke und Services über identitätsbasierte Zugriffskontrolle. Besonders geeignet ist die Technologie für mobile Mitarbeiter, die in gemeinsam genutzten Büroräumen des öffentlichen Sektors auf Informations- und Kommunikationsservices zugreifen.

TrustSec bietet eine Reihe von integrierten Services für Routing- und Switching-Produkte von Cisco, die Benutzerzugriffe auf Netzwerke absichern, Datenverkehr im Netzwerk schützen und über zentrale Überwachungsfunktionen, Fehlerbehebung und Reporting-Funktionen verfügen. Zu diesen gehören:

- **Identitätsbasierte Zugriffskontrolle** – für rollenbasierten Zugriff. Geräte, die die Richtlinien nicht erfüllen, können unter Quarantäne gestellt oder repariert werden. Gegebenenfalls kann der Zugriff auch vollständig verweigert werden.
- **Gastbenutzerzugang** – autorisierte Gäste erhalten über ein individuell anpassbares Webportal eingeschränkten Zugriff auf spezifische Ressourcen wie beispielsweise Internet oder Drucker. Jeglicher interner Netzwerkzugriff wird gesperrt. Zudem werden alle Aktivitäten dokumentiert.

- **Datenintegrität und Vertraulichkeit** – Datenpfade können via MACsec vom Endgerät bis zum Netzwerkkern verschlüsselt werden. Dabei bleibt die Sichtbarkeit von Datenströmen in wichtigen Netzwerkanwendungen (z. B. Firewalls, IPSs, QoS-Engines etc.) erhalten.
- **Überwachung, Verwaltung und Fehlerbehebung** – zentralisierte, richtlinienbasierte Überwachung und Tracking von Benutzern und Geräten. Umfassende Fehlerbehebung, detaillierte Überprüfung sowie Verlaufs- und Echtzeitberichte.

In Cisco TrustSec sind diese Funktionen über verschiedenste identitätsspezifische Zugriffs-, Authentifizierungs-, Autorisierungs- und weitere Netzwerkservices enthalten.

## Cisco AnyConnect Secure Mobility Solution

Der Cisco AnyConnect Client wurde konzipiert, um eine sichere, richtlinienbasierte Zugriffskontrolle für mobile Mitarbeiter zu ermöglichen.

Cisco AnyConnect stellt eine Erweiterung der herkömmlichen VPN-Clients mit Software für Remote-Zugriff dar. Es kann seine Netzwerk-Betriebsumgebung erkennen und eine Richtlinienentscheidung darüber treffen, wo es eingesetzt wird – zum Beispiel im LAN der Hauptniederlassung, in dem einer Zweigstelle, in einem Heimnetzwerk oder über einen Wireless-Hotspot. Der AnyConnect-Client hat dadurch die Möglichkeit, automatisch das integrierte VPN zu nutzen, falls kein Office-LAN verfügbar ist. Auf diese Weise wird gewährleistet, dass der Remote-Zugriff auf Anwendungen und Services sicher abläuft.

So ist es mobilen Mitarbeitern möglich, von jedem beliebigen Ort zu arbeiten, ohne manuell einen VPN-Client starten zu müssen.

Der Cisco AnyConnect Client unterstützt eine Vielzahl an mobilen Geräten wie Notebooks (Kompatibilität mit Windows 7 ist gegeben) und Smartphones. Der Client verwendet das effizienteste VPN-Tunneling-Protokoll und ist die erste VPN-Lösung mit Datagram Transport Layer Security (DTLS)-Protokoll. Er ist nahtlos kompatibel mit Cisco ASA. Die Verbindung von Client und Appliance bietet die optimale Kombination aus client-seitigen Sicherheitsrichtlinien und zentralisierter Firewall mit Inhaltsüberwachung.

## Wie kann Cisco Sie unterstützen?

Cisco hat über Jahre hinweg aktiv zur Entwicklung von IT-Sicherheitslösungen beigetragen.

Wir bieten ein breites Portfolio an Sicherheitslösungen. Zudem sind Sicherheitsfunktionen ein fester Bestandteil unserer wichtigsten Netzwerkprodukte. Diese Produkte werden weltweit in die Netzwerke von Service Providern und Kunden implementiert. Dadurch hat Cisco einzigartige Möglichkeiten, Informationen über IT-Sicherheit zu erfassen. Mithilfe von Security Intelligence Operations (SIO) erhalten wir beispielsweise Informationen über die Bedrohungen, mit denen sich unsere Kunden konfrontiert sehen und können auf diese proaktiv eingehen.

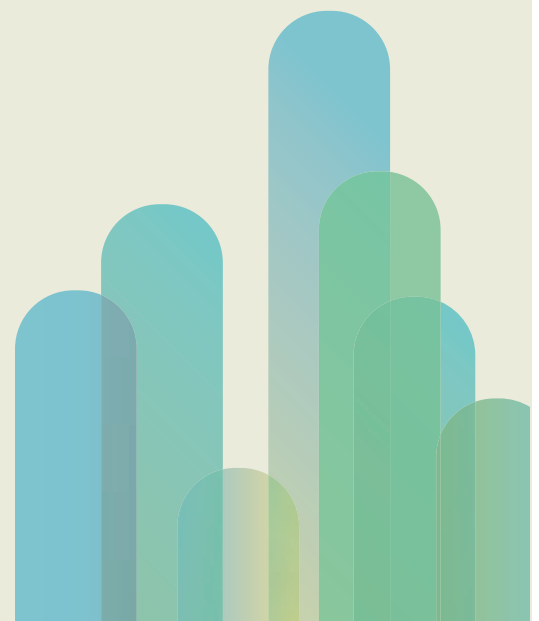
Neben Technologien bietet Cisco auch Consulting-Services für Cyber-Security. Gerne beraten wir Sie bei der Umsetzung von Empfehlungen aus diesem Whitepaper unter Berücksichtigung Ihrer Technologie- und Sicherheitsstrategie. Auch wenn es um die optimale Umsetzung Ihrer Sicherheitsstrategie geht, stehen wir Ihnen beratend zur Seite.

Erwarten Sie von uns, dass wir Sie auf flexible und innovative Art und Weise bei der Entwicklung Ihrer IT-Sicherheitsmaßnahmen unterstützen. So zum Beispiel durch:

- Unterstützung bei der Entwicklung von Sicherheitsstrategien
- Durchführung von Sicherheitsanalysen Ihrer Infrastruktur
- Beratung hinsichtlich des Lebenszyklus von Technologien zur Behebung von Sicherheitsschwachstellen und Identifizierung von Potentialen zur Kostensenkung
- Entwicklung von Übergangsplänen zur Verbesserung der Sicherheitsfunktionen entsprechend geschäftlicher Anforderungen und neuen Lösungsmodellen
- Beratung zur optimalen Implementierung von Sicherheitstechnologien für die Netzwerkbasis und von Lösungen der vier Sicherheitslayer
- Unterstützung bei der Definition und Umsetzung der Information Assurance-Ziele

Wir freuen uns darauf, die Inhalte dieses Whitepapers persönlich mit Ihnen zu besprechen. Zur näheren Erörterung Ihrer individuellen Anforderungen wenden Sie sich bitte an Ihren Cisco Ansprechpartner vor Ort.

„Nutzen Sie unser Fachwissen in allen Aspekten der Sicherheitstechnologie.“



## Weitere Informationen

Die folgenden Referenzmaterialien enthalten weiterführende Informationen.

### **Cisco Borderless Networks**

<http://www.cisco.de/borderless>

### **Cisco SecureX Architektur**

<http://www.cisco.com/web/DE/products/securex/index.html>

### **Sicherheit an der Netzwerkbasis - „Turn It On“-Programm**

[http://www.cisco.com/web/strategy/government/usfed\\_tio.html](http://www.cisco.com/web/strategy/government/usfed_tio.html)

### **Cisco ASA Security Appliances**

[http://www.cisco.com/web/DE/verticals/smb/products/security/asa\\_5500\\_series\\_adaptive\\_security\\_appliances.html](http://www.cisco.com/web/DE/verticals/smb/products/security/asa_5500_series_adaptive_security_appliances.html)

### **Cisco IPS Sensor Appliances**

<http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/index.html>

### **Cisco Ironport E-Mail und Web Security Appliances**

<http://www.cisco.com/en/US/products/ps10154/index.html>

<http://www.cisco.com/en/US/products/ps10164/index.html>

### **Cisco VPN Encryption Solutions (DMVPN und GET-VPN)**

<http://www.cisco.com/en/US/products/ps6658/index.html>

<http://www.cisco.com/en/US/products/ps7180/index.html>

### **Cisco TrustSec**

[http://www.cisco.com/web/DE/pdfs/borderless/C45\\_577269\\_trustsec.pdf](http://www.cisco.com/web/DE/pdfs/borderless/C45_577269_trustsec.pdf)

### **Cisco AnyConnect Secure Mobility Solution**

[http://www.cisco.com/web/DE/solutions/mobility\\_index.html](http://www.cisco.com/web/DE/solutions/mobility_index.html)



---

**Hauptgeschäftsstelle  
Nord- und Südamerika**  
Cisco Systems, Inc.  
San Jose, CA

**Hauptgeschäftsstelle  
Asien/Pazifik**  
Cisco Systems (USA) Pte. Ltd.  
Singapur

**Hauptgeschäftsstelle  
Europa**  
Cisco Systems International BV Amsterdam,  
Niederlande



---

Cisco unterhält weltweit mehr als 200 Niederlassungen. Die Adressen mit Telefon- und Faxnummern finden Sie auf der Cisco Website unter [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco und das Cisco Logo sind Marken von Cisco Systems, Inc. und/oder Partnerunternehmen in den Vereinigten Staaten und anderen Ländern. Eine Liste der Cisco Marken finden Sie unter [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Die genannten Marken anderer Anbieter sind Eigentum der jeweiligen Inhaber. Die Verwendung des Begriffs „Partner“ impliziert keine gesellschaftsrechtliche Beziehung zwischen Cisco und anderen Unternehmen. (1005R) C02-640572-00 1/11