successstory

Sicherheit für die Diplomatie: Schutz von Botschaftsnetzen

secunet

Der konsequente Einsatz starker Kryptographie, gepaart mit einem Schlüsselmanagement, das die Zugriffe auf Daten regelt, sind die einzige Methode sich bereits heute vor Bedrohungen wie Stuxnet und wikileaks zu schützen.

Dr. Rainer Baumgart, CEO secunet, Behörden Spiegel 2011

herausforderung

Die Außenministerien vieler Nationen sind die zentrale Stelle für nationale Diplomatie und vertreten einen Staat mit ihren Botschaften und Konsulaten im Ausland. Vertrauliche und je nach außenpolitischer Lage auch kritische Informationen fließen dabei über Ländergrenzen hinweg.

Für Dritte häufig von hohem Interesse, können deren Veröffentlichung ernste Folgen für Diplomaten oder sogar das Heimatland haben. Deshalb bedürfen diese Daten eines besonderen Schutzes und ihre Verfügbarkeit muss jederzeit und überall sichergestellt sein. Die Anforderungen an Botschaftsdaten und ihre Netze sind hoch und vielfältig:

- Sichere Bearbeitung, Speicherung und Übertragung der Daten
- Schnelle und sichere Kommunikation auch in Regionen mit besonderen politischen oder infrastrukturellen Gegebenheiten
- Hohe Verfügbarkeit per DSL, ISDN, Standleitung oder Satellit
- Reduzierung der Netzkosten
- Integration vieler unterschiedlicher Anwendungen und Dienste
- Einfache Inbetriebnahme in den ausländischen Vertretungen auch ohne IT-Spezialisten
- Umgang mit unterschiedlich eingestuften Dokumenten (Need-to-know)

vorteile

- Von vielen Staaten Zulassung für höchste nationale Geheimhaltungsstufen
- Hochsichere Übertragung aller Daten
- Nutzung aller IP-fähigen Übertragungskanäle z. B. Internet
- Auch in Gebieten mit schwacher Provider-Infrastruktur möglich, z. B. per Satellit
- Einsatzbereit auch unter klimatisch extremen Bedingungen
- Modellabhängiger Abstrahl- und Manipulationsschutz
- Notlöschfunktion für den Ernstfall
- Bereitstellung aller notwendigen Informationen für alle Mitarbeiter
- Zeitgleiche Information an alle Botschaften weltweit
- Keine Erfordernis von IT-Know-how in den Standorten
- Versandmöglichkeit mit kommerziellen Transportdiensten in allen Geheimhaltungsstufen
- Technik Made in Germany

Wie wir Sie unterstützen können...

Wenn Sie Ihr Botschaftnetz sichern wollen, können Sie aus verschiedenen Optionen hinsichtlich Redundanz, Datendurchsatz, Abstrahlschutz u. a. wählen. Erfahrene secunet Berater unterstützen Sie gern, die für Sie beste Lösung zusammen zu stellen.

Ein typisches SINA Netz für ein Außenministerium zur sicheren Datenübertragung, VoIP und Videokonferenzen könnte wie folgt aussehen:

- ✔ n x SINA L3 Box S 30M für jede Botschaft. Unsere kompakteste SINA L3 Box ist ideal für Standorte mit geringen Bandbreiten.
- ✔ 2 x SINA L3 Box S 200M für die Zentrale. Diese SINA L3 Box hat mit bis zu 200 MBit/s einen deutlich höheren Datendurchsatz und kann redundant ausgelegt werden.
- ✔ 1 x SINA Management: Das SINA Management ermöglicht die zentrale Administration aller SINA Komponenten aus der Zentrale im Heimatland.
- ✔ n x SINA Workstation für reisende Mitarbeiter. Die SINA Workstation bietet Schutz für Ihre Daten, online und offline.
- ✔ 1 Woche SINA Training für Ihre Administratoren

Gern beraten wir Sie in allen Aspekten der IT-Sicherheit, von der Netzwerkplanung bis zu Integration und Rollout.

lösung: Zehn Jahre Erfahrung in der Absicherung von Botschaftsnetzen

Viele Außenministerien vertrauen die IT-Sicherheit ihrer weltweit verteilten diplomatischen Vertretungen seit Jahren der secunet an. Dabei setzt secunet in allen betreuten Botschaftsnetzen die gemeinsam mit dem BSI entwickelte sichere Inter-Netzwerk Architektur SINA ein. Diese Architektur ermöglicht die sichere Bearbeitung, Speicherung und Übertragung von vertraulichen Informationen über offene Netze. SINA entstand aus dem Anspruch, Lösungen zu schaffen, die den hohen Sicherheitsanforderungen von Ministerien, Behörden und der Verteidigung gerecht werden.

Die Sicherung und Sicherstellung der elektronischen Kommunikation, ob über Leased Lines, Internet oder Satellit, kann mit SINA kostenoptimiert in jedem Land der Welt, angepasst an die vorhandene Infrastruktur, realisiert werden. So lässt sich jedes IP-fähige Netz zur Datenübertragung bis TOP SECRET nutzen.

Ein Rollenkonzept steuert die Zugriffsmöglichkeiten aller autorisierten Mitarbeiter. Eine einheitliche Infrastruktur kann verschieden eingestufte Daten – von offen bis TOP SECRET – strikt voneinander trennen, so dass auch jeder Amtsmitarbeiter nur sieht, was für ihn bestimmt ist. Innerhalb dieser Rollenkonzepte lassen sich Sonderrechte definieren, die zum Beispiel dem Botschafter den Zugang zu allen Informationen für seinen jeweiligen Zuständigkeitsbereich ermöglichen.

Die tägliche Arbeit in Botschaften und Konsulaten erfordern zudem eine hohe Mobilität. Diese Mobilität stellt gleichzeitig besondere Anforderungen an die ITK-Ausstattung. Auch hier hat Sicherheit oberste Priorität, die mit SINA auch in mobilen Arbeitsumgebungen gegeben ist.

Eine wichtige Rolle spielen Botschaften und Konsulate bei der Visa- und Passbeantragung. secunet begleitet und berät seit vielen Jahren die Bundespolizei sowie internationale Organisationen wie die ICAO bei der Entwicklung neuer Standards insbesondere von biometrischen Merkmalen in hoheitlichen Dokumenten. Die international eingesetzten Lösungen der secunet umfassen alle Phasen des eID Lebenszyklus – von der Beantragung und Datenerfassung über deren Produktion und Ausgabe bis hin zur Anwendung bei der Identitätsprüfung sowie der Rückführung der Dokumente.

umsetzung

Sichere Datenanbindung der Botschaften

Zentral für die Arbeit der Botschaften auf der ganzen Welt sind die laufende Abstimmung und der Informationsaustausch mit der Zentrale im Heimatland. Dabei werden auch viele besonders schützenswerte Daten auf elektronischem Weg übermittelt.

Mit dem Einsatz von SINA sind Mitlesen, Manipulieren oder Umleiten der Informationen zu keinem Zeitpunkt möglich, da der gesamte Datenstrom verschlüsselt übertragen wird. Dieser Schutz wird durch eine Virtual Private Network-Lösung (VPN) realisiert, die zwischen den Standorten besteht und für den schnellen Austausch vertraulicher und geheimer Nachrichten auch über das öffentliche Internet geeignet ist. Jede Vertretung wird dazu mit einer SINA L3 Box ausgestattet, die für die Verschlüsselung der Daten und den Verbindungsaufbau im VPN zuständig ist.

Die SINA L3 Box ist ein Gateway, das selbst kein Schlüsselmaterial oder kryptographische Funktionen enthält. Erst in Verbindung mit einer Smartcard und einer PIN können die Daten im Netzwerk ver- und entschlüsselt werden. Daher kann die SINA L3 Box auch ohne Einschränkungen gelagert und mit kommerziellen Versendern verschickt werden. Muss die Botschaft im Notfall verlassen werden, stellt die zurückgebliebene Box kein Sicherheitsrisiko dar: Je nach Modell genügt das Abziehen der Smartcard bzw. die Aktivierung einer Notlöschtaste.

SINA®

Bundesamt
für Sicherheit in der
Informationstechnik

*SINA ist eine gemeinsame Entwicklung von BSI und secunet

Sichere Mobilität

Neben der sicheren Netzanbindung mit SINA L3 Boxen ermöglicht die SINA Produktpalette auch die sichere Ausstattung von reisenden Mitarbeitern, Heimarbeitsplätzen, Honorarkonsuln und Büros, die nicht zum Ministeriums- oder Botschaftsgelände gehören. Für einen stationären Einsatz eignet sich der SINA Terminal. Ein festplattenloser Rechner, der nur als Ein- und Ausgabeterminal dient und ein Abbild der Daten am Monitor anzeigt. Die Daten selbst verbleiben jederzeit auf Servern in der Zentrale. SINA Terminal ist ausgelegt für die Datenübertragung aller Einstufungen. Auch hier greift das Rollenkonzept und erlaubt nur vorher definierte Zugriffe auf Daten.

Mobile Mitarbeiter können mit der SINA Workstation auf ein Notebook vertrauen, mit dem sie auch unterwegs Daten sicher bearbeiten, speichern und übertragen können. Anders als beim SINA Terminal können Daten auch lokal auf der verschlüsselten Festplatte abgelegt werden. Über jede Verbindung, auch von einem öffentlichen Hot Spot oder per Satellit, wird eine sichere VPN-Verbindung ins SINA Netz aufgebaut.

Sichere Telefonie

Innerhalb des SINA Netzes können auch Telefonate oder Videokonferenzen verschlüsselt geführt werden. Telefoniert wird per Voice over IP (VoIP), so dass keine Kosten für gesicherte Telefonleitungen entstehen. In der SINA Workstation sind modellabhängig die beiden Software-Funktionen Telefonie und Videokonferenz bereits standardmäßig vorinstalliert. Die Botschaftsmitarbeiter können über jeden Internetanschluss weltweit einfach mit einem an das Notebook angeschlossenen Headset telefonieren – stets geschützt vor unerwünschten Mithörern im Netz.

erfolg

Außenministerien, die ihre weltweite Botschaftsvernetzung mit secunet realisiert haben, konnten nicht nur die Kosten für die Vernetzung senken, sondern auch die Zusammenarbeit der Standorte verbessern und Arbeitsprozesse beschleunigen. Dabei muss Informationssicherheit und Hochverfügbarkeit bei gleichzeitiger Kosteneinsparung kein Widerspruch sein. Einzelne Kunden bezifferten die Einsparungen seit dem Einsatz von SINA auf bis zu 75 %: Die Benutzung öffentlicher Netze für den Aufbau eines Botschaftsnetzes macht den teuren Einsatz von botschaftseigenen Standleitungen überflüssig. Der Einsatz von VoIP über das SINA Netz macht Telefonate nicht nur abhörsicher, sondern auch deutlich günstiger als über eine geschützte Leitung. Allein bereits die Kommunikationskosten können für ein mit SINA gesichertes Botschaftsnetz nachhaltig gesenkt werden.

Kostensenkend können sich auch Einsatzumgebung sowie Maintenance und vereinfachte Rollout-Szenarien auswirken: Modellabhängig ist die SINA L3 Box abstrahl- und manipulationsgeschützt und erfordert daher keine besonders geschützte Umgebung oder Räume (z. B. Faradayscher Käfig). Sie kann in gewöhnlichen Büros aufgestellt und auch von Mitarbeitern ohne besondere IT-Kenntnisse in Betrieb genommen werden. Die Inbetriebnahme und Administration des Systems werden bequem online durch die IT-Abteilung im Heimatland übernommen.

secunet Security Networks AG

secunet, seit 2004 Sicherheitspartner der Bundesrepublik Deutschland, ist einer der führenden Anbieter anspruchsvoller IT-Sicherheit. Im engen Dialog mit seinen nationalen und internationalen Kunden aus Privatwirtschaft sowie öffentlichen Institutionen entwickelt secunet leistungsfähige Produkte und fortschrittliche IT-Sicherheitslösungen. Damit schützt secunet nicht nur die IT-Prozesse und -Systeme seiner Kunden, sondern erzielt intelligente Prozessoptimierungen und schafft nachhaltige Mehrwerte.

Bei secunet konzentrieren sich mehr als 380 Experten auf Themen wie Kryptographie (SINA), E-Government, Kritische Infrastrukturen sowie Business- und Automotive-Security – mit dem Anspruch, in Qualität und Technik immer einen Schritt voraus zu sein. Unser Ziel ist der effiziente und effektive Schutz der Daten und IT-Infrastrukturen bis hin zur Absicherung des geistigen Eigentums und der Reputation unserer Kunden.

secunet Security Networks AG
Kurfürstenstraße 58
45138 Essen
Tel.: +49-201-5454-0
Fax: +49-201-5454-1000
E-Mail: info@secunet.com
www.secunet.com

04/2016