Bundesamt
für Sicherheit in der
Informationstechnik

Sichere Inter-Netzwerk Architektur

SINA

Ein Projekt im Auftrag des BSI mit secunet

Inhaltsverzeichnis

Unsere Gesellschaft auf dem Daten-Highway

Wir befinden uns heute in einer globalen Informationsgesellschaft. Immer komplexere, schnellere und weltweit vernetzte informationstechnische Systeme übernehmen zunehmend weitreichendere Aufgaben.

Die Informationstechnik (IT) hat inzwischen alle gesellschaftlichen Bereiche erfasst und ist ein selbstverständlicher und teilweise unsichtbarer Bestandteil des Alltags geworden.

Die Funktionsweise von informationstechnischen Produkten und Systemen ist aber für weite Kreise der Anwender nicht sofort und ohne fundiertes Fachwissen durchschaubar. Vertrauen in die Informationstechnik kann aber nur dann entstehen, wenn sich die Nutzer auf ihre Anwendung verlassen können. Das gilt insbesondere für die Sicherheit von Daten im Hinblick auf Vertraulichkeit, Verfügbarkeit und Integrität.

Um einen sicheren Umgang mit Daten und informationsverarbeitenden Systemen zu gewährleisten, ist es erforderlich, entsprechend der jeweiligen Gefährdungslage Sicherheitsstandards zu entwickeln und einzuhalten.

Das BSI im Dienst der Öffentlichkeit

Das Bundesamt für Sicherheit in der Informationstechnik wurde am 1. Januar 1991 mit Sitz in Bonn gegründet und gehört zum Geschäftsbereich des Bundesministeriums des Innern.

Mit seinen derzeit rund 550 Mitarbeiterinnen und Mitarbeitern und 62 Mio. Euro Haushaltsvolumen ist das BSI eine unabhängige und neutrale Stelle für alle Fragen zur IT-Sicherheit in der Informationsgesellschaft.

Als zentraler IT-Sicherheitsdienstleister des Bundes ist das BSI operativ für den Bund, kooperativ mit der Wirtschaft und informativ für den Bürger tätig.

Durch die Grundlagenarbeit im Bereich der IT-Sicherheit übernimmt das BSI als nationale IT-Sicherheitsbehörde Verantwortung für unsere Gesellschaft und ist dadurch eine tragende Säule der Inneren Sicherheit in Deutschland.

Ziel des BSI ist der sichere Einsatz von Informations- und Kommunikationstechnik in unserer Gesellschaft. IT-Sicherheit soll als wichtiges Thema wahrgenommen und eigenverantwortlich umgesetzt werden. Sicherheitsaspekte sollen schon bei der Entwicklung von IT-Systemen und -Anwendungen berücksichtigt werden.

Das BSI wendet sich mit seinem Angebot an die Anwender und Hersteller von Informationstechnik. Zielgruppe sind die öffentlichen Verwaltungen in Bund, Ländern und Kommunen sowie Privatanwender und Unternehmen.

Diese Broschüre gibt einen Überblick über die sichere Inter-Netzwerk-Architektur (SINA) des BSI. Es werden die technischen Hintergründe, die potenziellen Angriffsvektoren und die Lösungen vorgestellt.

1 Sichere Inter-Netzwerk Architektur (SINA)

1 Sichere Inter-Netzwerk Architektur (SINA)

Der Name SINA steht für Sichere Inter-Netzwerk Architektur und beinhaltet Komponenten zur geschützten Bearbeitung, Speicherung und Übertragung von Verschlusssachen (VS) über das Internet. Die SINA-Produktfamilie enthält die einzigen vom Bundesamt für Sicherheit in der Informationstechnik (BSI) bis zum höchsten nationalen Einstufungsgrad STRENG GEHEIM zugelassenen IP-basierten Kryptosysteme.

Schwerpunkt der SINA-Produktfamilie ist der Schutz von elektronischen Informationen vor unberechtigtem Zugriff. Die Gewährleistung dieses Schutzes ist eine Kernaufgabe jeder IT-Sicherheitsvorsorge und unverzichtbare Grundvoraussetzung bei der Umsetzung einer Sicherheitspolitik.

Bei der Verarbeitung von elektronischen Informationen ist es daher zwingend erforderlich, alle gesetzlichen und regulativen Vorgaben einzuhalten. Bei einer unberechtigten Weitergabe oder Veröffentlichung von Geheimnissen drohen im schlimmsten Fall beträchtliche existenzbedrohende Schäden für die jeweilige Organisation.

In der Informationstechnik wird die Einhaltung von gesetzlichen, unternehmensinternen und vertraglichen Vorgaben durch den Bereich „IT-Compliance“ beschrieben. Die Produkte der SINA-Familie stellen ein Instrument dar, um den Schutz von Informationen gemäß den geltenden Vorgaben durchzusetzen.

Die SINA-Komponenten bilden einen Baukasten zur Realisierung von elektronischen VS-Systemen.

1.1 Vertrauenswürdige Übertragung: die SINA L3 Box

Für die gesicherte Übertragung von Verschlusssachen über ungesicherte Netze stellt die SINA L3 Box ein Virtual Private Network (VPN) zur Verfügung. Dadurch können Verschlusssachen mit hohem Schutzbedarf sicher und wirtschaftlich über bestehende, nicht vertrauenswürdige Verbindungen (beispielsweise über das Internet) transportiert werden. Die SINA L3 Box sorgt durch eine für den Benutzer transparente Verschlüsselung für einen angemessenen Schutz der Vertraulichkeit und stellt somit einen bewährten und unverzichtbaren Baustein zur Realisierung von elektronischen VS-Systemen mit hohem Schutzbedarf dar.

1.2 Ein Safe für schützenswerte Daten: der SINA Storage Service

Der SINA Storage Service ist für das zentrale Speichern der Verschlusssachen in einem Netzwerk zuständig. Die Daten werden verschlüsselt abgelegt und sind dadurch geschützt, wie in einem Safe. Das Entschlüsseln der Daten ist nur durch Personen möglich, die die Informationen zur Erledigung ihrer Arbeit benötigen. Dadurch wird das Prinzip „Kenntnis, nur wenn nötig“ konsequent und ohne Kompromisse für die Sicherheit umgesetzt. Der SINA Storage Service befindet sich zurzeit noch in der Entwicklung.

1.3 Revisionssichere Nachweise: der SINA Audit Service

Verlässliche Nachweise werden durch den SINA Audit Service erbracht. Diese Komponente leistet somit einen wichtigen Beitrag für die IT-Compliance, da für eine Arbeit mit Verschlusssachen verlässliche Nachweise zwingend vorgeschrieben sind. Der SINA Audit Service hat die Aufgabe, diese Nachweise revisionssicher zu protokollieren.

1.4 Geordnetes Ablegen und Verwalten: der SINA Registry Service

Nachvollziehbares Verwaltungshandeln spielt auch bei der Bearbeitung von Verschlusssachen eine wichtige Rolle. Der SINA Registry Service ist die Komponente zum geordneten Ablegen und Identifizieren von Verschlusssachen. Mit dieser Komponente werden die sogenannten Metadaten verwaltet, also die Einstufung der Verschlusssachen, der Hersteller oder das Gültigkeitsdatum. Der SINA Registry Service erlaubt auch das Gruppieren von Verschlusssachen zu Akten und Vorgängen, ermöglicht nachvollziehbare und verbindliche Mitzeichnungen und stellt den Benutzern die benötigten Verzeichnisse (beispielsweise das Bestandsverzeichnis oder das Quittungsbuch) zur Verfügung.

1.5 Sicherer Arbeitsplatz: die SINA Workstation

Mit der SINA Workstation steht ein sicherer Arbeitsplatz zur Erstellung und Bearbeitung von Verschlusssachen bis zum Einstufungsgrad GEHEIM zur Verfügung. Die SINA Workstation bietet ein ganzheitliches Sicherheitskonzept: von der Festplattenverschlüsselung über eine Schnittstellenkontrolle bis hin zu einer sicheren Anbindung über ein VPN zu einem vertrauenswürdigen Netz. Darüber hinaus sichert die SINA Workstation eine verlässliche Separation unterschiedlich eingestufter Arbeitsplätze auf nur einer physikalischen Hardware zu. Neben einer stationären Desktop-Variante existieren auch mobile Versionen auf der Basis von Laptops.

2 Angriffsvektoren und Gefährdungen

2 Angriffsvektoren und Gefährdungen

Unter Angriffsvektoren versteht man die unterschiedlichen Wege und Techniken, mit deren Hilfe ein Angreifer in ein Computersystem eindringen und danach für seine Zwecke missbrauchen kann. Meistens werden dazu bekannt gewordene Sicherheitslücken in dem anzugreifenden System verwendet. Häufig werden solche Angriffsvektoren durch gezieltes Einbringen von Schadsoftware ausgenutzt. Die folgenden Abschnitte beschreiben einige dieser Angriffsvektoren.

2.1 Einbringen von Schadsoftware über E-Mails

Das Einbringen von Schadsoftware über E-Mails geschieht durch das unbeabsichtigte und unwissentliche Öffnen manipulierter E-Mail-Anhänge durch den Benutzer. Durch diese Methode kann alleine durch das Öffnen eben dieser speziell präparierten Anhänge der Arbeitsplatz unbemerkt mit Schadsoftware infiziert werden. Dabei werden in erster Linie Sicherheitslücken der zur Darstellung der E-Mail-Anhänge benötigten Anwendungen (z. B. PDF-Betrachter und Office-Anwendungen) als Einfallstor genutzt. Die Gefahr einer Infektion mit Schadsoftware durch manipulierte E-Mail-Anhänge ist nach wie vor sehr hoch.

2.2 Einbringen von Schadsoftware über Drive-by-Downloads

Ein Drive-by-Download ist das unbeabsichtigte und unwissentliche Herunterladen von Software auf den Rechner eines Benutzers. Durch diese Methode kann alleine durch das Betrachten von speziell präparierten Web-Seiten der Arbeitsplatz unbemerkt mit Schadsoftware infiziert werden. Dabei werden in erster Linie Sicherheitslücken des Web-Browsers ausgenutzt. Die Gefahr einer Infektion mit Schadsoftware durch Drive-by-Downloads ist hoch und nimmt stetig zu.

2.3 Einbringen von Schadsoftware über Datenträger

Das Einbringen von Schadsoftware über Datenträger geschieht durch das unbeabsichtigte und unwissentliche Öffnen manipulierter Dateien, die sich auf einem mobilen Datenträger (z. B. USB-Speicherstick) befinden. Zusätzlich kann auch der Datenträger selbst manipuliert werden, unabhängig von den auf ihm gespeicherten Inhalten. Durch diese Methoden kann alleine durch den Anschluss des präparierten Datenträgers der Arbeitsplatz unbemerkt mit Schadsoftware infiziert werden. Dabei werden in erster Linie Sicherheitslücken der zur Darstellung der auf dem Datenträger gespeicherten Dateien benötigten Anwendungen (z. B. PDF-Betrachter und Office-Anwendungen) oder Lücken im Betriebssystem bei der Einbindung mobiler Datenträger in das lokale Dateisystem ausgenutzt. Die Gefahr einer Infektion mit Schadsoftware durch präparierte Datenträger ist nach wie vor hoch und in einzelnen Fällen sogar besonders kritisch (siehe z. B. die Angriffe mittels der Schadsoftware Stuxnet).

2.4 Einbringen von Schadsoftware über einen WLAN-Hot-Spot

Eine erhöhte Gefährdung besteht, wenn Clients auch in Netzen anderer Betreiber, insbesondere an Hot Spots, betrieben werden. Um das Web-Portal von Hot Spots zu erreichen, müssen die Ports für DHCP, HTTP und gegebenenfalls auch DNS für alle IP-Adressen freigeschaltet sein. Zudem erfolgt die Anmeldung am Hot Spot häufig über eine Web-Oberfläche, die aktive Inhalte verwendet. Um sich anzumelden, müssen aktive Inhalte zugelassen werden. Durch die direkte, in der Regel unverschlüsselte Kommunikation mit dem Hot Spot bietet der Client eine größere Angriffsfläche zum Einbringen von Schadsoftware.

2.5 Direkter Angriff auf das Gerät

Mobile Arbeitsplätze werden in der Regel in nicht-vertrauenswürdigen Umgebungen betrieben. Dies ermöglicht unbefugten Personen einen direkten Angriff auf das Endgerät. Erlangt eine

unbefugte Person unbemerkt vom Anwender, Zugang zum Endgerät, kann sie Daten entwenden oder Daten bzw. Binär-Dateien manipulieren. Hierzu muss sich das Endgerät nicht unbedingt im Besitz des Angreifers befinden. Der logische Zugang kann über eine bestehende Internetverbindung oder direkten physikalischen Zugriff erfolgen.

3 Nutzungsszenarien

3 Nutzungsszenarien

Ein VPN ist heutzutage ein etabliertes Verfahren, um über fremde Netze schützenswerte Daten auf eine sichere Art und Weise zu übermitteln. Mithilfe eines VPNs kann somit die Wirtschaftlichkeit eines fremden Transportnetzes mit der Sicherheit einer eigenen dedizierten Verbindung kombiniert werden. Dabei lassen sich grundsätzlich die Szenarien

» Remote Access über beliebige Netze und

» Separation von Netzen

unterscheiden.

3.1 Remote Access über beliebige Netze

Zunehmend wird die Möglichkeit geschaffen, dass Mitarbeiter Teile ihrer Arbeit außerhalb der Firmengebäude verrichten können. Vor dem Hintergrund der wachsenden Bedrohungslage stellen diese Anforderungen die bestehenden IT-Infrastrukturen vor teilweise neue Sicherheitsherausforderungen. Um den Schutz von Daten weiterhin gewährleisten zu können, kann sich nicht mehr vollständig auf die sichere und vertrauenswürdige Umgebung der Arbeitsstelle verlassen werden. Durch zahlreiche Angriffsmöglichkeiten sind die Vertraulichkeit, die Integrität, die Verfügbarkeit und die Authentizität der auf den mobilen Geräten befindlichen schützenswerten Daten bedroht.

Zur Abwehr dieser identifizierten Angriffe müssen geeignete Arbeitsplätze zumindest

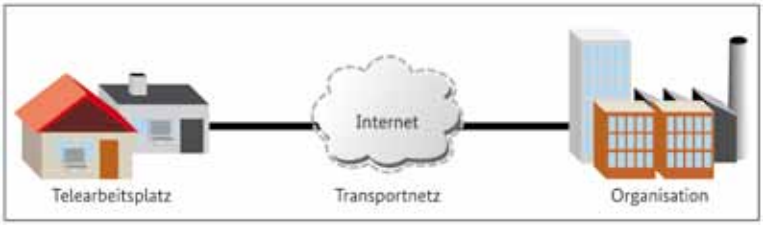
» einen verschlüsselten Kommunikationskanal zum Firmennetzwerk,

» eine Verschlüsselung aller lokalen Daten und

» eine Kontrolle von Peripheriegeräten und Schnittstellen

als sicherheitsspezifische Funktionen enthalten. Die Stärke dieser sicherheitsspezifischen Funktionen sowie ihre Unumgehbarkeit sind maßgeblich für den Schutz der IT-Infrastrukturen vor Angriffen.

3.1.1 Telearbeitsplätze bzw. mobiles Arbeiten innerhalb vertrauenswürdiger Umgebungen

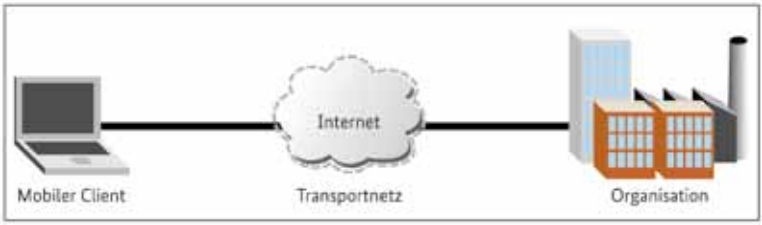


Bei diesem Einsatzfall bearbeitet ein Nutzer seine Daten an unterschiedlichen Orten, die jeweils einen erhöhten Schutz zur Verfügung stellen. Die in den Einsatzorten verfügbare Infrastruktur muss einerseits einen materiellen Schutz, beispielsweise gegen Diebstahl, und andererseits eine vertrauenswürdige Netzinfrastruktur aufweisen. Durch das Vorhandensein von Firewalls und Paketfiltern in der vertrauenswürdigen Netzinfrastruktur kann beispielsweise ein erhöhter Schutz für den mobilen Arbeitsplatz gewährleistet werden. Der Transport des ausgeschalteten Geräts erfolgt grundsätzlich durch den Nutzer selbst bzw. durch Personen, die Kenntnis vom Inhalt der Daten erlangen dürfen. Eine Lagerung außerhalb des sicheren Einsatzortes ist nicht zulässig. Dieses Szenario ist beispielsweise relevant für Nutzer, die ihre Arbeit in unterschiedlichen Niederlassungen einer Firma verrichten müssen.

Beispiel: Ein Mitarbeiter nutzt das Arbeitszimmer in seiner privaten Wohnung, um einen zusätzlichen, vollwertigen und sicheren Arbeitsplatz zu realisieren. Der Arbeitsplatz in seiner privaten Wohnung ergänzt den Arbeitsplatz im Unternehmen.

Beispiel: Eine Servicemitarbeiterin betreut viele Niederlassungen des Unternehmens. In jeder Niederlassung steht ihr ein Arbeitsplatz zur Verfügung.

3.1.2 Mobile Arbeitsplätze



Mobile Arbeitsplätze ermöglichen das Arbeiten an unterschiedlichsten Orten. Zur Verbindung in die unternehmenseigene Infrastruktur können beispielsweise Mobilfunknetze (UMTS/GPRS) oder WLAN-Hot-Spots genutzt werden. Das für die Verbindung genutzte öffentliche Netz leistet keinen Beitrag zum Schutz der transportierten Daten bzw. des angeschlossenen Gerätes.

Zusätzlich muss das ausgeschaltete Gerät beispielsweise in einem Hotelzimmer unbeaufsichtigt gelagert werden können.

Zu einer vollständigen elektronischen Bürokommunikation gehört neben dem Bearbeiten von Dokumenten und E-Mails in der Regel auch eine verlässlich geschützte Sprachkommunikation. Mobile Arbeitsplätze können zu diesem Zweck spezielle Programme zur Verfügung stellen, die den mobilen Arbeitsplatz in ein vollständiges VoIP-Telefon verwandelt. Besonderen Schutz sollte hierbei die Vertraulichkeit und Integrität der übertragenen Gespräche genießen.

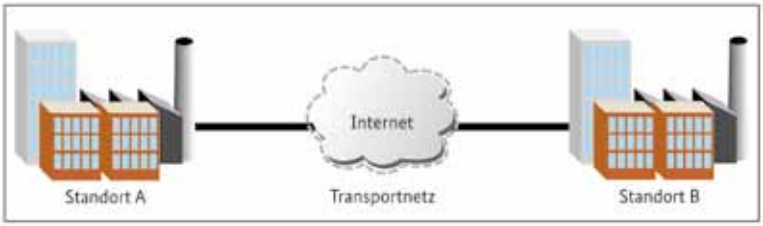
Beispiel: Eine Mitarbeiterin nutzt einen WLAN-Hot-Spot in einem Hotelzimmer, um mit ihrem Laptop an einer Telefonkonferenz teilzunehmen.

Beispiel: Ein Außendienstmitarbeiter nutzt den WLAN-Hot-Spot in einem Hotel, um mit seinem Unternehmen kommunizieren zu können.

Beispiel: Eine Mitarbeiterin nutzt einen privaten DSL-Zugang, um berufliche E-Mails oder Dokumente zu bearbeiten.

Beispiel: Auf dem Flughafen verbindet sich ein Mitarbeiter mit Hilfe von UMTS mit seinem Unternehmen, um auf die aktuelle Version einer Präsentation zuzugreifen.

3.1.3 Verbinden von Standorten



In der Praxis verteilen sich speziell größere Unternehmen oder Behörden auf mehrere Standorte. Diese unterschiedlichen Standorte müssen an eine organisationseigene IT-Infrastruktur angeschlossen werden. Aus Gründen der Wirtschaftlichkeit werden für diesen Anschluss in der Regel Netze von speziellen Netzanbietern genutzt. Die zu transportierenden Daten oder die IT-Infrastrukturen der Unternehmen bzw. Behörden erfahren durch diese Transportnetze keinen besonderen Schutz. Für die sichere Kopplung von verschiedenen Standorten bzw. Rechenzentren sind somit zusätzliche IT-Komponenten notwendig, um den Schutz der Daten oder IT-Infrastrukturen sicherzustellen.

Beispiel: Eine Behörde möchte zur Steigerung der Verfügbarkeit ihrer IT-Infrastrukturen eine redundante Verteilung der Dienste auf verschiedene, räumlich getrennte Rechenzentren realisieren. Da zur Erbringung der Dienste bei Ausfall eines Rechenzentrums in der Regel weiterhin alle Daten zur Verfügung gestellt werden müssen, ist eine Kopplung von Rechenzentren in einem solchen Fall notwendig.

3.2 Separation von Netzen

Heute besitzt fast jeder Arbeitsplatz eine Möglichkeit, auf das Internet zuzugreifen. Durch diese Zugriffsmöglichkeit wird allerdings der Arbeitsplatz mitsamt allen schützenswerten Daten den vollen Gefahren einer Internetnutzung ausgesetzt. Jeder Besuch einer WWW-Seite kann schon zur Infektion des Arbeitsplatzes und somit in finaler Konsequenz auch zum Verlust von wertvollen, schützenswerten Daten führen oder sogar das gesamte Netzwerk gefährden. Eine möglichst vollständige Separation von Unternehmens- bzw. Behördennetz vom Internet ist eine Grundvoraussetzung, um Angriffe aus dem Internet zu minimieren. Dabei muss neben der Separation auf der Netzwerkebene auch eine Separation auf dem Endsystem gewährleistet sein. Produkte zur Separation müssen somit neben dem verlässlichen Schutz durch Trennung auch eine sichere Konsolidierung auf einem einzigen Arbeitsplatz ermöglichen.

Beispiel: Eine Behörde möchte das Arbeitsnetz, in dem schützenswerte Daten enthalten sind, möglichst komplett vom Internet trennen. Bei der Trennung soll unter Beibehaltung der kompletten Funktionen des Arbeitsplatzes das Risiko eines Datenverlustes oder die Infektion des Behördennetzes minimiert werden.

3.3 Angriffsmatrix

Anwendbarkeit des Angriffsvektors	Telearbeitsplätze	Mobile Arbeitsplätze	Verbinden von Rechenzentren	Separation von Netzen
Schadsoftware über E-Mails	✓	✓	–	–
Schadsoftware über Drive-by-Download	✓	✓	–	–
Schadsoftware über Datenträger	✓	✓	–	–
Schadsoftware über WLAN-Hot-Spot	–	✓	–	–
Direkter Angriff auf das Gerät	✓	✓	✓	✓

4 Grundkonzepte der Sicherheit

4 Grundkonzepte der Sicherheit

4.1 Verschlüsselter Kommunikationskanal (Virtual Private Network)

Ein Virtual Private Network (VPN) stellt einen sicheren, verschlüsselten Kommunikationskanal zwischen zwei vertrauenswürdigen Netzen dar. Durch diesen sicheren Kanal werden die vertrauenswürdigen Netze vor Angriffen aus dem nicht vertrauenswürdigen Transportnetz geschützt.

4.2 Verschlüsselung lokaler Daten

Die Verschlüsselung lokaler Daten ist notwendig, da bei Verlust des Endgerätes eine unbefugte Kenntnisnahme der Daten verhindert werden muss.

4.3 Peripheriegerätekontrolle/Schnittstellenkontrolle

Die Peripheriegeräte- und Schnittstellenkontrolle stellt eine Ergänzung zum VPN dar. Sie verhindert, dass beispielsweise unabsichtlich der VPN-Tunnel durch Nutzung anderer Schnittstellen umgangen werden kann. Die zu kontrollierenden Schnittstellen sind unter anderem USB, kabelgebundene oder kabellose Netzwerk-Schnittstellen.

4.4 Trennung von Sicherheitsfunktionen und Client-Betriebssystem

Die Trennung von Sicherheitsfunktionen und Client-Betriebssystem stellt kein zwingend gefordertes Sicherheitsmerkmal dar, ist hier aber dennoch aufgeführt, um auf die Abhängigkeit der Sicherheitsfunktionen und dem Client-Betriebssystem hinzuweisen. Sind Sicherheitsfunktionen und Client-Betriebssystem nicht ausreichend getrennt, so stellen sie aus Sicher-

heitssicht eine Einheit dar, die gemeinsam bei der Evaluierung der Sicherheitsfunktion betrachtet werden muss. Dies schränkt die Flexibilität bei der Wahl des Client-Betriebssystems ein und muss auch bei der Update-Strategie des Client-Betriebssystems berücksichtigt werden. Sind jedoch Sicherheitsfunktionen vom Client-Betriebssystem ausreichend voneinander getrennt, so herrscht eine größere Flexibilität bei der Wahl des Client-Betriebssystems.

Ein zusätzlicher Vorteil bei der Trennung von Sicherheitsfunktionen und Client-Betriebssystem ist der einfachere Nachweis der Funktion und Stärke der Sicherheitsfunktionen.

5 Produkte

5 Produkte

SINA L3 Box

Verschlüsselung Kommunikationskanal ✓

Zulassung des BSI bis GEHEIM ✓

» VPN Gateway z.B. zur Kopplung von Rechenzentren über öffentliche Netze

» Kryptographische Gegenstelle für SINA Terminal bzw. SINA Workstation

» Datendurchsatz bis maximal 3 GBit/s (abhängig von Gerätetyp)

» Redundanz und Hochverfügbarkeitsmechanismen

SINA Workstation

Verschlüsselung Kommunikationskanal ✓

Verschlüsselung der lokalen Daten/Festplatte ✓

Kontrolle Peripheriegeräte/ Schnittstellen ✓

Zulassung des BSI bis GEHEIM
(bis VS-V auf marktgängigen Laptops/PCs) ✓

» Betrieb mehrerer (unterschiedlich eingestufter) Arbeitsplätze in einem System durch Virtualisierung

» Unterstützung unterschiedlicher Gastbetriebssysteme (z.B. Windows 7, aktuelle Linux-Distributionen)

» Zusätzlich integrierte Thin-Client-Technologie

» Integriertes VoIP-Telefon (Software) mit verschlüsseltem Kommunikationskannal

» Nutzung stationär (Desktop) oder mobil (Laptop)

SINA Terminal

Verschlüsselung Kommunikationskanal ✓

Kontrolle Peripheriegeräte/ Schnittstellen ✓

Zulassung des BSI bis GEHEIM ✓

» Betrieb mehrerer (unterschiedlich eingestufter) Arbeitsplätze in einem System durch Nutzung von Thin-Client-Technologie

» Integriertes VoIP-Telefon (Software) mit verschlüsseltem Kommunikationskannal

SINA Workflow (in Entwicklung)

Data Loss Prevention ✓

Enterprise Content Management ✓

Vorschriftenkonforme Nachweise ✓

Zulassung des BSI bis GEHEIM (geplant) ✓

» Vorschriftenkonforme Verarbeitung von Verschlusssachen

» Kryptografische Ablage und Zugriffsschutz der zu schützenden Daten mit dem SINA Storage Service

» Vorschriftenkonforme Nachweise mit dem SINA Audit Service

» Geordnetes Ablegen und Verwalten mit dem SINA Registry Service

» Unterstützung von kollaborativen Prozessen zum gemeinsamen Erstellen von Dokumenten

» Durchsetzen der existierenden normativen Sicherheitsvorgaben

6 Glossar

6 Glossar

Client

Ein Client stellt in der Client-Server-Architektur die Komponente dar, die Anfragen an den Server richtet. Ein Client kann im Sprachgebrauch sowohl ein Programm oder auch der komplette Computer sein.

Ethernet

Kabelgebundene Netzwerktechnologie für lokale Datennetze.

Gastbetriebssystem

Betriebssystem, das in einer virtuellen Maschine läuft.

Gateway

Ein Gateway oder auch Protokollumsetzer erlaubt es Netzwerke, die auf völlig unterschiedlichen Protokollen basieren, zu verbinden. Heute werden Gateways meistens durch Router realisiert.

Hot Spot

Unter dem Begriff Hot Spot werden öffentliche, drahtlose Internetzugänge bezeichnet, die meist gegen Bezahlung genutzt werden können. Hot Spots findet man häufig in Hotels, Restaurants oder Cafes.

Internet Protokoll (IP)

Das Internet Protokoll ist ein für die Vernetzung von Computern weitverbreitetes Netzwerkprotokoll und stellt die Basis für die Datenübertragung im Internet dar.

Kryptografisches Gateway (VPN-Gateway)

Vermittler, der durch Verschlüsselung und verschieden Sicherheitsmechanismen einen Datenaustausch zwischen Netzwerken gewährleistet.

Rechnernetzwerk

Ein Rechnernetzwerk (oder auch kurz Netzwerk genannt) ist ein Verbund von verschiedenen, primär selbstständigen elektronischen Systemen, wie beispielsweise Computern. Ziel eines Rechnernetzwerks ist die Etablierung der Kommunikation der einzelnen Systeme untereinander. Das Internet ist der bekannteste Vertreter eines Rechnernetzwerkes.

Rotes Netzwerk

Ein rotes Netzwerk ist ein Rechnernetz, das schützenswerte Informationen enthält. Um den Schutz dieser Informationen zuzusichern, muss das Netzwerk besondere Sicherheitsfunktionen umsetzen, um die gewünschte Vertrauenswürdigkeit zu erlangen. Ein rotes Netzwerk wird aus Sicht der Organisation als sicheres Netzwerk angesehen.

Router

Router sind Netzwerkgeräte, die verschiedene Netzwerke miteinander koppeln. Als Kopplungselement hat ein Router – je nach Sichtweise – die Aufgabe, die verschiedenen Netzwerke zu verbinden bzw. zu separieren. Aufgabe des Routers ist es IP-Pakete

an andere, angeschlossene Netzwerke zu leiten oder aber auch fehlgeleitete IP-Pakete zu blockieren.

Schwarzes Netzwerk

Ein schwarzes Netzwerk ist ein Rechnernetz, in das keine schützenswerten Informationen einer Organisation gelangen dürfen. Ein schwarzes Netzwerk wird aus Sicht der Organisation als unsicheres Netzwerk angesehen. Das Internet stellt ein schwarzes Netzwerk dar.

Server

Ein Server stellt in der Client-Server-Architektur die Komponente dar, die die Anfragen der Clients bearbeitet und beantwortet. Ein Server kann im Sprachgebrauch sowohl ein Programm oder auch der komplette Computer sein.

Thin Client

Ein Thin Client ist eine Komponente in der Client-Server-Architektur. Sie ist in einem Rechnernetz ein spezielles Endgerät (Terminal), das lediglich die Schnittstelle zum Benutzer darstellt (Eingabe und Ausgabe). Die Speicherung und Verarbeitung der Daten erfolgt ausschließlich auf einer Server-Komponente.

Verschlusssachen

Verschlusssachen sind im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse unabhängig von ihrer Darstellungsform (beispielsweise Schriftstücke, elektronische Dateien und Datenträger oder das gesprochene Wort). Sie werden entsprechend ihrer Schutzbedürftigkeit von einer amtlichen Stelle oder auf deren Veranlassung in Geheimhaltungsgrade eingestuft.

Voice over IP (VoIP)

Telefonieübertragung über IP-basierte Netzwerke, insbesondere über das Internet.

WLAN

Wireless Local Area Network ist ein lokales Funknetz zur Realisierung von Rechnernetzen.

Impressum

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik – BSI
53133 Bonn

Bezugsquelle
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185-189
53133 Bonn
E-Mail: sina@bsi.bund.de
bsi@bsi.bund.de
Internet: www.bsi.bund.de/SINA
Telefon: +49 (0) 22899 9582 - 0
Telefax: +49 (0) 22899 9582 - 5400

Stand
Februar 2013

Druck
Druckpartner Moser Druck + Verlag GmbH
53359 Rheinbach

Texte und Redaktion
Bundesamt für Sicherheit in der Informationstechnik – BSI

Artikelnummer
BSI-Bro13/322