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 600 Mitarbeiterinnen und Mitarbeitern und ca. 80 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)

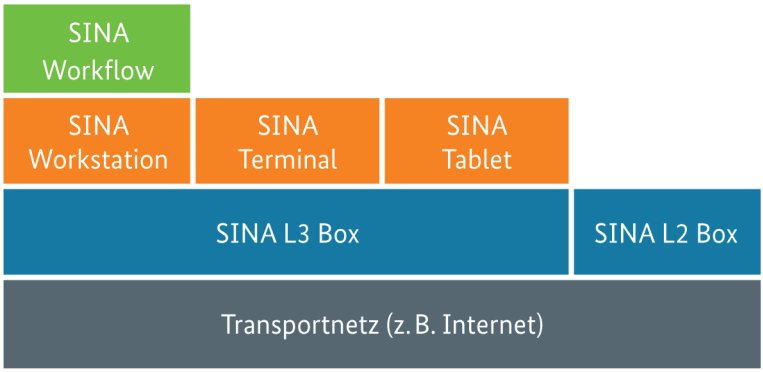
Der Name SINA steht für **S**ichere **I**nter-**N**etzwerk **A**rchitektur und beinhaltet Komponenten zur geschützten Bearbeitung, Speicherung und Übertragung von Verschlusssachen (VS) über das Internet. Die SINA-Produktfamilie wird seit dem Jahr 2000 entwickelt und enthält die einzigen vom Bundesamt 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 geheimhaltungsbedürftigen Informationen ist es zwingend erforderlich, alle gesetzlichen und regulativen Vorgaben einzuhalten. Bei einer unberechtigten Weitergabe oder Veröffentlichung von Geheimnissen drohen im schlimmsten Fall 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 des nationalen Geheimschutzes, der Verschlusssachenanweisung und der internationalen EU- und NATO-Vorgaben durchzusetzen.

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



1.1 Grundprinzipien des SINA-Designs

Ziel der SINA-Produktfamilie ist die Erhöhung des tatsächlichen IT-Sicherheitsniveaus in Behörden und Unternehmen. Eine angemessene Balance zwischen Sicherheit und Benutzbarkeit in SINA-Produkten ist dafür eine essentielle Voraussetzung.

Für die Benutzbarkeit von SINA Workstation, SINA Terminal und SINA Tablet jedes Einstufungsgrades ist ein Aspekt zentral: der Anwender möchte geheimhaltungsbedürftige Informationen in den gewohnten, kommerziellen Betriebssystemen und Softwareprodukten wie z. B. Office-Umgebungen bearbeiten können – obwohl diese keine Zulassung für die Bearbeitung von Verschlusssachen besitzen.

Diesen scheinbaren Widerspruch löst die gesamte SINA-Produktfamilie durch zwei Grundprinzipien auf:

1. SINA-Sicherheitsfunktionen sind für den Nutzer und seine Software unsichtbar (bzw. „transparent“)

2. SINA-Sicherheitsfunktionen sind durch den Nutzer und seine Software unumgehbar (Zwangssicherheit)

Diese Grundprinzipien werden auf verschiedenen Ebenen angewendet:

» Netzwerkverschlüsselung

» Festplattenverschlüsselung

» Schnittstellenkontrolle

» Separation von Sicherheitskomponenten und nicht-vertrauenswürdigen Komponenten

Zusätzlich ist es auf SINA Workstation, SINA Terminal und SINA Tablet möglich, auf demselben Endgerät mehrere Arbeitsumgebungen mit unterschiedlichen Einstufungsgraden parallel zu nutzen. Hier stellt SINA eine vertrauenswürdige Trennung und Informationsflusskontrolle zwischen den Arbeitsumgebungen zur Verfügung.

Nähere Informationen finden sich im Folgenden, insbesondere in Abschnitt 4 „Grundkonzepte der Sicherheit“.

1.2 Vertrauenswürdige Übertragung: SINA L3 Box und SINA L2 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.

Auch die **SINA L2 Box** ermöglicht eine gesicherte Kommunikation über bestehende, nicht vertrauenswürdige Verbindungen. Als Ethernet-Verschlüsseler agiert die SINA L2 Box auf einer tieferen Netzwerkschicht als die SINA L3 Box, wodurch u.a. ein höherer Datendurchsatz erzielt werden kann.

1.3 Sicherer Arbeitsplatz: SINA Workstation, SINA Terminal und SINA Tablet

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.

Die SINA Workstation ist sowohl in einer stationären Desktop-Variante als auch auf Basis von Laptops verfügbar. Daneben existiert mit dem **SINA Tablet** eine Tabletcomputer-Variante sowie mit dem **SINA Terminal** eine Thin-Client-Variante.

1.4 Geordnetes Ablegen und Verwalten: SINA Workflow

Nachvollziehbares Verwaltungshandeln spielt auch bei der Bearbeitung von Verschlusssachen eine wichtige Rolle. Der **SINA Workflow** 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 Workflow 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. Verlässliche Nachweise werden ebenfalls durch den SINA Workflow erbracht. Diese Komponente leistet somit einen wichtigen Beitrag für die IT-Compliance im Bereich Geheimschutz, da für eine Arbeit mit Verschlusssachen verlässliche Nachweise zwingend vorgeschrieben sind. SINA Workflow basiert auf einer kryptografischen Verschlüsselung der elektronischen Verschlusssachen. Das Produkt stellt somit eine verlässliche Zugriffskontrolle bereit, so dass die Kenntnisnahme von Verschlusssachen dem Bedarf entsprechend festgelegt und gesteuert werden kann.

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 weiterhin hoch.

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.

2.4 Einbringen von Schadsoftware über einen WLAN-Hot-Spot

Eine erhöhte Gefährdung besteht, wenn Clients auch in Netzen anderer Betreiber, insbesondere an WLAN-Hot-Spots, betrieben werden. Um das Web-Portal von Hot-Spots zu erreichen, müssen sich die Clients auch gegenüber fremden, in Reichweite befindlichen, Rechnern offenbaren. Zudem erfolgt die Anmeldung am Hot-Spot häufig über eine Web-Oberfläche, die aktive Inhalte verwendet. Durch die direkte, in der Regel unverschlüs-

selte 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 Hardware und Daten entwenden oder manipulieren. Für den Zugriff auf Daten muss sich das Endgerät nicht unbedingt im Besitz des Angreifers befinden. Der logische Zugang kann auch über eine bestehende Internetverbindung erfolgen.

2.6 Advanced Persistent Threat (APT)

Unter Advanced Persistent Threat („fortgeschrittene, andauernde Bedrohung“) versteht man zielgerichtete, hochprofessionelle Angriffe auf kritische IT-Infrastrukturen, Behörden oder Großunternehmen (siehe z. B. Angriff auf die IT des Bundestages 2015). Da APTs oft von staatlichen Akteuren mit beträchtlichen Ressourcen ausgehen, sind für die Abwehr von APTs gute Sicherheitsmaßnahmen und -prozesse eine Grundvoraussetzung. Vor dem Hintergrund der zunehmenden Digitalisierung der Gesellschaft nimmt die Gefahr und das Schadenspotenzial durch APTs stetig zu.

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. Im Bereich VPN lassen sich grundsätzlich die Szenarien

» Remote Access (Fernzugriff) über beliebige Netze und

» Separation von Netzen

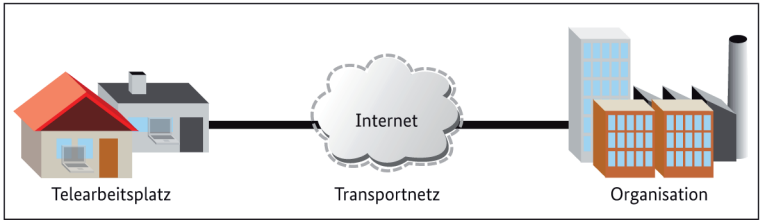
unterscheiden.

3.1 Remote Access über beliebige Netze

Klassischerweise befinden sich alle IT-Systeme innerhalb eines sicheren Perimeters, und die wenigen Konnektionspunkte zur Außenwelt werden mit Firewalls abgesichert. Mit dem zunehmenden Trend zur Vernetzung und zum mobilen Arbeiten ist jedoch ein klassischer Perimeterschutz immer schwieriger zu erreichen. So verrichten Mitarbeiter zunehmend Teile ihrer Arbeit außerhalb der Firmengebäude. Um den Schutz von Daten weiterhin gewährleisten zu können, kann man sich somit nicht mehr alleine auf die sichere und vertrauenswürdige Umgebung der Arbeitsstelle verlassen. Gerade vor dem Hintergrund der wachsenden Bedrohungslage stellt dies die bestehenden IT-Infrastrukturen vor neuen Sicherheitsherausforderungen. Durch zahlreiche Angriffsmöglichkeiten sind die Vertraulichkeit, die Integrität, die Verfügbarkeit und die Authentizität der schützenswerten Daten auf den sich außerhalb der Firmengebäude befindlichen Geräte bedroht.

Zur Abwehr von Angriffen müssen geeignete Arbeitsplätze zumindest die sicherheitsspezifischen Funktionen enthalten, welche in Abschnitt 1 angesprochen wurden und in Abschnitt 4 ausführlich beschrieben werden. 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 vertrauter Umgebungen

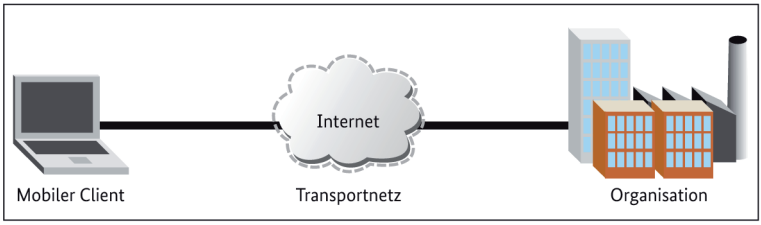


Bei diesem Einsatzfall bearbeitet ein Nutzer seine Daten wiederkehrend in dedizierten Räumlichkeiten. Diese Räumlichkeiten können im Vergleich zu dem Szenario „mobile Arbeit“ eine erhöhte Umgebungssicherheit gewährleisten. Dabei ist ein relevanter Aspekt der materielle Schutz, beispielsweise gegen Diebstahl bei Transport, Nutzung und Lagerung. Der zweite relevante Aspekt ist der Schutz vor IT-Angriffen, welcher durch eine vertrauenswürdige und hinreichend gesicherte Netzinfrastruktur sichergestellt werden muss.

Beispiel: Ein Mitarbeiter nutzt das Arbeitszimmer in seiner privaten Wohnung, um mit der SINA Workstation 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 in nicht vertrauenswürdigen Umgebungen



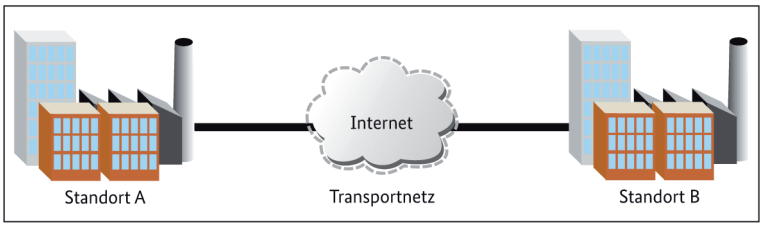
Mobile Arbeitsplätze ermöglichen das Arbeiten an den unterschiedlichsten Orten. Zur Verbindung in die unternehmenseigene Infrastruktur können beispielsweise Mobilfunknetze (UMTS/GPRS) oder WLAN-Hot-Spots genutzt werden. Das für die Verbindung genutzte öffentliche Netz leistet keinen Beitrag zum Schutz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

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

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

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 die Netze von 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. Damit trotz Ausfall eines Rechenzentrums noch alle Dienste und Daten verfügbar sind, ist eine sichere Kopplung von Rechenzentren 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 wichtige Maßnahme, um einen möglichen Schaden durch Angriffe aus dem Internet zu minimieren. Dabei muss neben der Separation auf der Netzwerkebene auch eine Separation auf dem Endsystem gewährleistet sein.

Beispiel: Eine Behörde möchte das Arbeitsnetz, in dem schützenswerte Daten enthalten sind, möglichst komplett vom Internet trennen, den Nutzern aber trotzdem am selben Endgerät einen vollen Internetzugriff ermöglichen. Bei der Trennung von Arbeitsnetz und Internet soll daher unter Beibehaltung der kompletten Funktionen des Arbeitsplatzes das Risiko eines Datenverlustes oder die Infektion des Behördennetzes minimiert werden.

4 Grundkonzepte der Sicherheit

4 Grundkonzepte der Sicherheit

Die grundlegenden IT-Sicherheitsziele sind die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität. Zur Wahrung dieser Ziele werden vielfältige Sicherheitskonzepte und -mechanismen eingesetzt, von denen einige in den folgenden Abschnitten beschrieben werden.

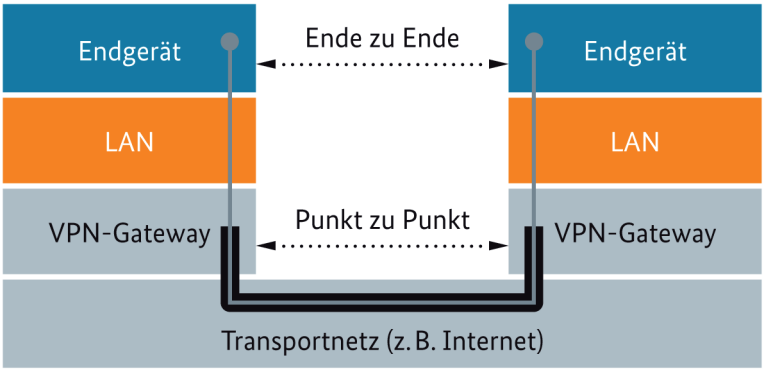
4.1 Verschlüsselter Kommunikationskanal (Virtual Private Network)

Ein Virtual Private Network (VPN) stellt einen sicheren, verschlüsselten Kommunikationskanal zwischen vertrauenswürdigen Netzen (Punkt-zu-Punkt) oder zwischen Endgeräten (Ende-zu-Ende) dar.

Allgemein bezeichnet man unsichere Netzwerke, in die keine schützenswerte Informationen gelangen dürfen, als schwarze Netzwerke. Als rote Netzwerke bezeichnet man als sicher angesehene Rechnernetze, in denen schützenswerte Informationen auch unverschlüsselt vorliegen dürfen. Das Internet stellt ein schwarzes Netzwerk dar, während die internen LANs einer Organisation je nach Ausprägung auch als rote Netzwerke angesehen werden können.

Traditionell sind VPN-Verbindungen Punkt-zu-Punkt-Verbindungen, d.h. die Verschlüsselung des Transportkanals erfolgt zwischen VPN-Gateways. Gegen Angriffe auf den verschlüsselten Transportkanal aus dem Transportnetz (schwarzes Netz) bietet eine Punkt-zu-Punkt-VPN-Verbindung bei korrekter Umsetzung ausreichenden Schutz. Jedoch werden die Daten in den sogenannten vertrauenswürdigen Netzen (LANs, rote Netze) hinter den jeweiligen Endpunkten unverschlüsselt wei-

tergeleitet und sind somit in der Regel nicht geschützt gegen Angriffe auf die Vertraulichkeit von Geräten oder Software, welche sich innerhalb des vertrauenswürdigen Netzes befinden. Werden die Endpunkte des VPN-Kanals in die kommunizierenden Endgeräte verschoben, so liegt eine Ende-zu-Ende-VPN-Verbindung vor. Bei einer konsequenten Nutzung von Ende-zu-Ende-VPN-Verbindungen werden Angriffe auf den Kommunikationskanal aus dem eigenen LAN deutlich erschwert.



4.2 Verschlüsselung lokaler Daten

Die Verschlüsselung lokaler Daten schützt vor einer ungewollten Kenntnisnahme bei Verlust des Endgerätes. Auch bei der Entsorgung oder dem Umtausch von Speichermedien stellt eine konsequente Verschlüsselung der lokalen Daten einen Schutz vor ungewollter Kenntnisnahme der Daten dar.

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 Schnitt-

stellen umgangen werden kann. Die zu kontrollierenden Schnittstellen sind unter anderem USB, kabelgebundene oder kabellose Netzwerk-Schnittstellen.

4.4 Trennung von Sicherheitsfunktionen und Client-Betriebssystem

Für eine Einschätzung des tatsächliches Schutzes durch Sicherheitsfunktionen ist die Trennung von Sicherheitsfunktionen und Client-Betriebssystem ein wichtiger Aspekt. Sicherheitsfunktionen, die im Client-Betriebssystem ausgeführt werden, können von Sicherheitsproblemen des Client-Betriebssystems umgangen werden. Sind Sicherheitsfunktionen und Client-Betriebssystem nicht ausreichend voneinander getrennt, so stellen sie aus Sicherheitssicht eine Einheit dar. Bei einer Bewertung der Sicherheitsfunktion müssen dann beide Komponenten als Einheit gemeinsam bewertet werden. Dies schränkt entweder die Wirksamkeit der Sicherheitsfunktion oder 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 getrennt, wie z. B. bei SINA Workstations der Fall, 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

Die im vorigen Abschnitt beschriebenen Grundkonzepte der Sicherheit sind in vollem Umfang in der SINA Produktpalette umgesetzt worden. Durch diese und weitere Sicherheitskonzepte wird effektiv einer großen Zahl von Bedrohungen begegnet, welche von ungewollter Kenntnisnahme bei Verlust oder Diebstahl des Endgeräts bis hin zu hochprofessionellen, zielgerichteten Angriffen reicht.

Die Trennung von Sicherheitsfunktionen und Client-Betriebssystemen wird in der SINA Produktfamilie unter anderem durch Virtualisierung sichergestellt. Hierbei dient ein auf Sicherheit optimiertes und mit vielfältigen Sicherheitsfunktionen ausgestattetes Linux-System als Basis (Host-Betriebssystem). Als Client-Betriebssystem (Gast-Betriebssystem) können beliebige Betriebssysteme, wie z. B. Windows oder aktuelle Linux-Distributionen, verwendet werden. Die Virtualisierung erfolgt transparent, so dass der Benutzer mit dem Client-Betriebssystem in gewohnter Weise interagiert. So können auch mit Schadsoftware kompromittierte Client-Betriebssysteme Daten nicht an den SINA-Sicherheitsfunktionen der Zwangsverschlüsselung vorbeileiten.

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 Workstation, SINA Terminal, SINA Tablet und SecuSUITE (abhängig von Produkttyp)

» Datendurchsatz maximal 5 GBit/s (abhängig von Gerätetyp, Stand 2016)

» Redundanz und Hochverfügbarkeitsmechanismen

SINA L2 Box

Verschlüsselung Kommunikationskanal ✓

Zulassung des BSI bis VS-NUR FÜR DEN DIENSTGEBRAUCH (GEHEIM für 2016/2017 erwartet) ✓

» Ethernet-Verschlüsseler z. B. zur Kopplung von Rechenzentren über öffentliche Netze

» Hochperformante, protokollunabhängige Verschlüsselung

» Kryptographische Gegenstelle für andere SINA L2 Boxen

» Datendurchsatz maximal 10 GBit/s (abhängig von Gerätetyp, Stand 2016)

» Redundanz und Hochverfügbarkeitsmechanismen

SINA Workstation

Verschlüsselung Kommunikationskanal ✓

Verschlüsselung der lokalen Daten/Festplatte ✓

Kontrolle Peripheriegeräte/ Schnittstellen ✓

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

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

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

» Zusätzlich integrierte Thin-Client-Technologie

» Verschlüsselte VoIP-Kommunikation

» Nutzung stationär (Desktop) oder mobil (Laptop)

SINA Tablet

Verschlüsselung Kommunikationskanal	✓
Verschlüsselung der lokalen Daten/Festplatte	✓
Kontrolle Peripheriegeräte/ Schnittstellen	✓
Zulassung des BSI bis VS-NUR FÜR DEN DIENST-GEBRAUCH	✓

» Vollständige Funktionalität der SINA Workstation mit einer an Touch-Bedienung angepassten Oberfläche

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

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

» Zusätzlich integrierte Thin-Client-Technologie

» Verschlüsselte VoIP-Kommunikation

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

» Verschlüsselte VoIP-Kommunikation

SINA Workflow

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

» automatisierte, vorschriftenkonforme Nachweise

» Geordnetes Ablegen und Verwalten

» Unterstützung von kollaborativen Prozessen zum gemeinsamen Erstellen von Dokumenten

» Durchsetzung 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 Cafés.

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.

LAN

Local Area Network ist ein lokales Netzwerk zur Realisierung von Rechnernetzen.

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 (VS)

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 einen der Geheimhaltungsgrade VS-NfD (Nur für den Dienstgebrauch), VS-V (Vertraulich), GEHEIM oder STRENG GEHEIM eingestuft.

Virtualisierung

Unter Virtualisierung versteht man im Kontext der SINA-Produkte das Nachbilden von Hardware durch eine Abstraktionsschicht aus Software. Es ist möglich Rechner, Speicher oder Netzwerke zu virtualisieren. Ein Beispiel für die Virtualisierung eines Rechners ist das Ausführen eines Betriebssystems (Gast) innerhalb eines anderen Betriebssystems (Host). Während der Host direkten Zugriff auf die Hardware des Rechners hat, kann der virtualisierte Gast nur indirekt über die Abstraktionsschicht aus Software auf Hardwareressourcen zugreifen.

Voice over IP (VoIP)

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

VPN-Gateway

Ein Virtual Private Network (VPN) Gateway ist ein Vermittler, der durch Verschlüsselung und verschiedene Sicherheitsmechanismen einen geschützten Datenaustausch zwischen Netzwerken gewährleistet. Üblicherweise handelt es sich dabei um ein physisches Gerät, es existieren aber auch virtualisierte VPN-Gateways.

WLAN

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

Impressum

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik – BSI

Bezugsquelle
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185-189
53175 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
Januar 2016

Druck
Druck- und Verlagshaus Zarbock GmbH & Co. KG
Sontraer Straße 6
63086 Frankfurt am Main
Internet: www.zarbock.de

Texte und Redaktion
Bundesamt für Sicherheit in der Informationstechnik – BSI

Bildnachweis
Titelseite: BSI, Seite 5: fotolia/kalafoto, Seite 6: BSI,
Grafiken: BSI, Produktfotos: secunet Security Networks AG

Artikelnummer
BSI-Bro16/322

www.bsi.bund.de