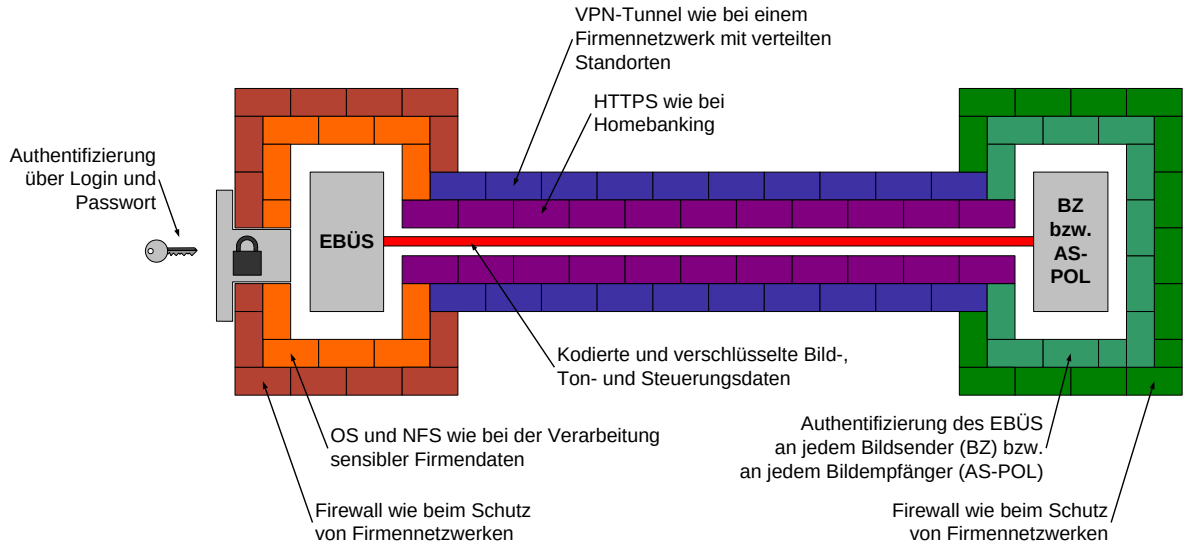
accellence

Datensicherheit bei EBÜS

Konzept für eine sichere Übertragungstechnik



Status: Entwurf, 03.08.2006

Inhalt

1 Einführung 3
2 Quellen 4
3 Grundlagen 5
4 ISDN 6
5 IP 7
6 VPN 8
7 VLAN 8
8 RS232 9
9 HTTPS 10
10 Verschlüsselung 10
11 Host-Tabelle 11
12 IP-Ports 11
13 Passwort 11
14 Separate Prozessräume 11
15 Sicheres Dateisystem 11
16 Sicherung gegen Fehlbedienung 12
17 Support / Hotline 12

1 Einführung

Je nach Einsatzgebiet ergeben sich mehr oder weniger hohe Anforderungen an die Datensicherheit: Bei einer rein lokalen Videoübertragung innerhalb eines privaten Netzes ohne Verbindungen nach außen braucht man sich um das Thema Datensicherheit wenig Sorgen zu machen; bei sicherheitskritischen Anwendungen mit Schnittstellen zu öffentlichen Netzen ist dagegen ein professionelles Sicherheitskonzept unverzichtbar.

EBÜS setzt auch beim Thema Datensicherheit auf Standards und auf hersteller-unabhängige Lösungen. EBÜS unterstützt eine große Bandbreite marktüblicher Übertragungstechnik-Komponenten, mit denen das Gesamtsystem je nach konkreten Erfordernissen bezüglich Kosten oder Sicherheit optimiert werden kann.

Für EBÜS gelten dabei die gleichen Regeln wie für andere IT-Systeme auch: Basis für sichere Systeme ist in erster Linie die Qualifikation derjenigen, die ein System einrichten und warten. Von der Netzwerkplanung bis zur laufenden Systemadministration wird zuverlässiges Personal benötigt, welches über umfassende Erfahrungen und aktuelles Wissen auf dem Gebiet der Netzwerksicherheit verfügt.

Von kompetenten Administratoren kann das System dann so eingerichtet werden, dass die Anwender auch durch (absichtliche oder unbeabsichtigte) Fehlbedienung keinen Schaden anrichten können.

Die erforderlichen Informationen, um IT-Systeme sicher einzurichten und zu betreiben, finden Sie unter den in Kapitel 2 angegebenen Quellen sowie in den weiteren Kapiteln dieses Dokumentes.

Es gibt heute eine Vielzahl von Verfahren, Software und Geräten, um IT-Netzwerke sicher zu machen. Auch um für künftige Innovationen offen zu sein legt EBÜS Sie nicht auf bestimmte Technologien fest, sondern überlässt es Ihrer Entscheidung, welche Sicherheitsvorkehrungen mit welchem Sicherheitslevel (und entsprechendem Kosten-/Zeitaufwand) Sie bei Ihrer EBÜS-Installation verwenden wollen.

Bei Fragen zu dieser Thematik stehen wir gern zu Ihrer Verfügung.

2 Quellen

Die maßgeblichen Regeln für sichere IT-Systeme werden in Deutschland vom "Bundesamt für Sicherheit in der Informationstechnik (BSI)" erarbeitet und laufend aktualisiert. Auf der Website www.bsi.de informiert es über sein Angebot und bietet umfassende aktuelle Informationen zum Thema Datensicherheit.

Des weiteren sind unbedingt die Sicherheitshinweise des Betriebssystem-Herstellers zu beachten. Es müssen regelmäßig Sicherheits-Updates vorgenommen werden, damit eventuelle Sicherheitslücken unverzüglich geschlossen werden. Die dazu benötigten Funktionen sind in aktuellen Betriebssystemen bereits eingebaut, müssen aber auch aktiviert und richtig bedient werden.

Weitere aktuelle Informationen zum Thema IT-Sicherheit bietet der Heise-Verlag unter www.heise.de/security/.

3 Grundlagen

Ein IT-Sicherheitskonzept muss folgende Punkte gewährleisten:

1. Authentizität: Die Daten stammen von einem zugelassenen Absender
2. Integrität: Die Daten wurden bei der Übertragung nicht verfälscht
3. Vertraulichkeit: Nur der vorgesehene Empfänger kann die Daten lesen
4. Zuverlässigkeit: Alle abgesendeten Daten kommen beim Empfänger an
5. Sicherheit: Abwehr von unerwünschten Eindringlingen (Hacker, Viren, ...)

Punkt 1 bis 3 können durch geeignete Verschlüsselungsverfahren erreicht werden. Punkt 4 kann durch redundante Übertragungswege (z.B. DSL + ISDN + UMTS) und eine verteilte Systemstruktur verbessert werden. Für Punkt 5 ist es erforderlich, dass gezielt nur die erwünschten Verbindungen zugelassen werden und alles andere durch Firewalls, Virenscanner etc. ferngehalten wird.

Am sichersten ist es, für die Videoübertragung ein völlig separates Netzwerk und separate PCs zu verwenden. Dann ist eine gegenseitige Beeinflussung von Videosystem und restlicher EDV-Technik ausgeschlossen.

Man kann mehrere autarke Arbeitsplätze aufbauen, die jeder für sich voll arbeitsfähig sind (Erhöhung der Zuverlässigkeit durch redundante Auslegung; Vermeiden eines "single point of failure", also einer zentralen Stelle, deren Ausfall das gesamte System lahm legt). Diese einzelnen Arbeitsplätze kann man durch entsprechende Netzwerk-Konfiguration unter "Quarantäne" stellen, so dass z.B. ein Virenbefall auf einem PC auf diesen begrenzt wird: Das Gesamtsystem bleibt mit den anderen autarken Arbeitsplätzen arbeitsfähig, während der befallene PC durch Neuinstallation auf Basis einer Sicherheitskopie der Festplatte repariert wird.

Diese Netzwerk-Entkopplung lässt sich mittels Technologien wie VLAN und VPN auch dann noch aufrecht erhalten, wenn (meist aus Kosten- oder Platzgründen) für die Videoübertragung die gleichen physikalischen Leitungen genutzt werden sollen wie für die restliche EDV-Technik, denn VLAN und VPN "tunneln" die Daten durch andere Übertragungsmedien hindurch, ohne dass es zu einer logischen Verbindung der Netzwerke kommt.

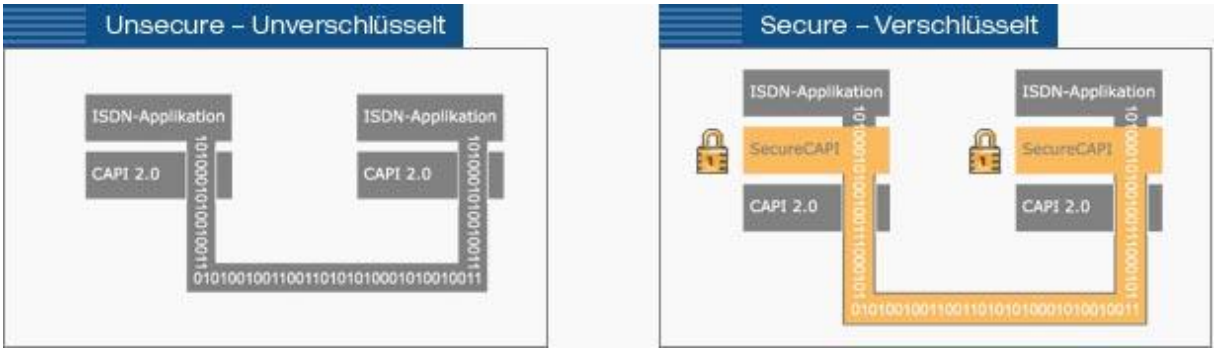
Manchmal ist jedoch eine logische Verbindung gewünscht (z.B. wenn Video-aufschaltungen automatisch auf Basis von Informationen erfolgen sollen, die nur in einem anderen EDV-System verfügbar sind). Dann ist diese Schnittstelle so auszulegen, dass nur die gewünschten Informationen übertragen werden können und fremde Daten keine Chance haben, diese Schnittstelle zu passieren. Dies kann z.B. durch eine RS232-Kopplung mit entsprechenden Filtern auf der Empfängerseite gewährleistet werden. EBÜS bietet entsprechende Module z.B. für die Kopplung mit Alarm-Management-Systemen.

Alle Übergänge von dem sicheren eigenen Netz zur unsicheren "Außenwelt" müssen geeignet abgesichert werden. Dazu mehr in den folgenden Kapiteln.

4 ISDN

Eine Datenübertragung über ISDN gilt vielen Anwendern als sicherer als eine IP-Verbindung, weil hier die Daten nur in einer direkten Punkt-zu-Punkt-Verbindung übertragen werden. Dennoch existieren auch hier Sicherheitsrisiken, weil diese Verbindungen über viele Kilometer Leitung und zahlreiche Schaltschränke geführt werden, an denen sie angezapft werden können. Die unverschlüsselten Daten können dann von Fremden leicht ausgelesen und ggf. manipuliert werden.

Um dem vorzubeugen, kann man Daten auch für den Transport über ISDN verschlüsseln. Entsprechende Tools bietet z.B. die Firma "active elements" (siehe www.securecapi.de).



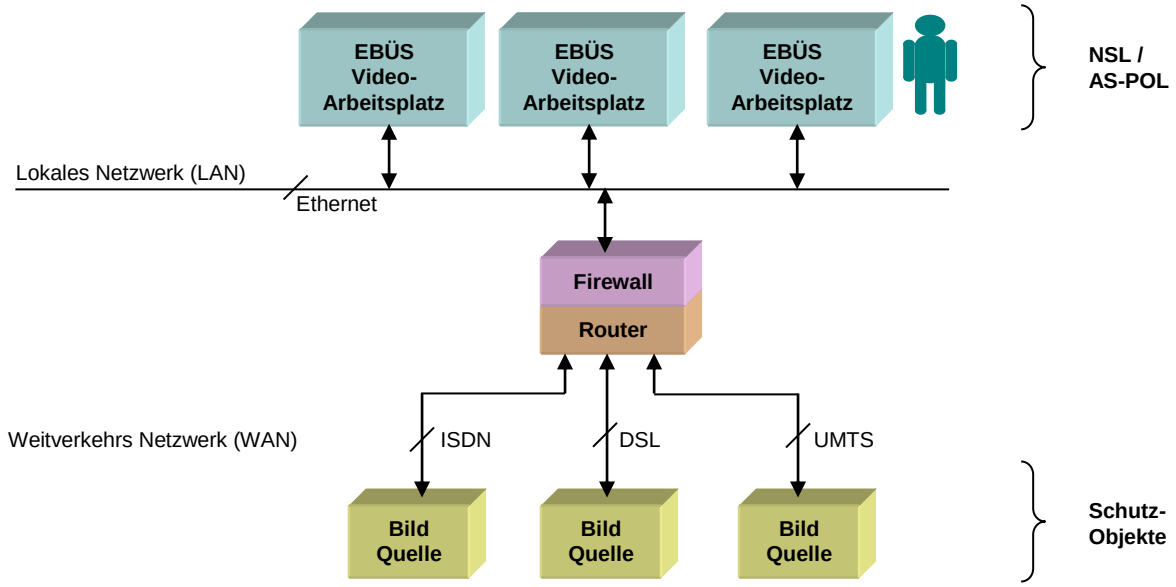
5 IP

Die Verwendung von IP (Internet-Protokoll) wird von vielen gleichgesetzt mit einer Internet-Verbindung. Zunächst sagt IP jedoch nur etwas darüber aus, in welchem Rahmenformat die Daten übertragen werden und nicht, über welchen physikalischen Übertragungsweg. Man kann z.B. Daten mittels IP auch über eine ISDN-Verbindung übertragen ("IP over ISDN"); das ist dann mindestens genau so sicher, als wenn man diese Daten direkt über ISDN übertragen würde.

IP hat sich weltweit als Standard-Protokoll durchgesetzt, mit dem alle Arten von elektronischen Daten in einem gemeinsamen Rahmenformat übertragen werden können. Entsprechend groß ist auch das Angebot an Sicherheitsprodukten für diese Technologie. Je nach Einsatzgebiet und konkreten Anforderungen müssen bei der Netzwerkplanung die passenden Sicherheitsprodukte vorgesehen werden, um einen angemessenen Schutz zu erreichen.

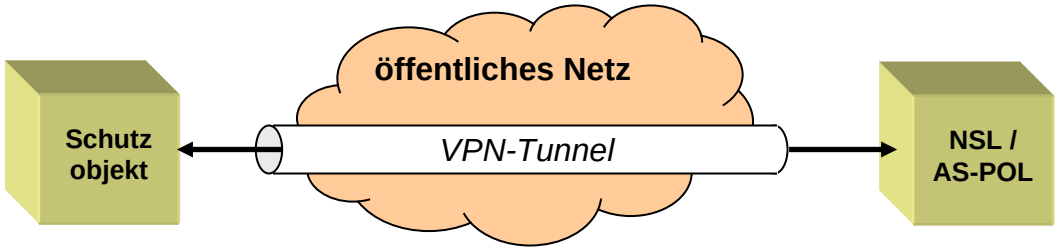
Zur Grundausrüstung gehören heute **Firewalls**, die so eingestellt werden müssen, dass nur die erwünschten Daten durchgelassen und alle fremden Zugriffe gesperrt werden.

Die Verbindung zwischen verschiedenen Netzwerk-Segmenten wird bei IP über sogenannte **Router** hergestellt. In Routing-Tabellen wird festgelegt, welche Datenverbindungen zugelassen werden sollen. Mittels NAT (network address translation) können moderne Router unerwünschte Zugriffe verhindern. Die Sicherheitsmerkmale und die fachgerechte Konfiguration der Router bilden somit einen entscheidenden Faktor im Sicherheitskonzept.



6 VPN

Wenn IP-Datenverkehr doch einmal über unsichere Wege erfolgen muss, so kann er mittels VPN-Technologie (virtual private network) gesichert werden: Ein VPN schafft durch das unsichere Medium hindurch einen sogenannten "Tunnel", durch den die sensiblen Daten transportiert werden können. Mittels Verschlüsselung, Prüfsummen und Sequenznummern gewährleistet das VPN die Authentizität, Integrität und Vertraulichkeit der Daten und verhindert ein Eindringen fremder Daten in den Tunnel.



Ein VPN ermöglicht auf diese Weise auch über öffentliche Netze Datenverbindungen, so als ob die Teilnehmer direkt miteinander verbunden wären; die Einflüsse des öffentlichen Netzes werden durch die VPN-Technologie abgeschirmt.

Die VPN-Technologie wird heute in vielen, auch sehr sensiblen Bereichen eingesetzt, und hat sich dort gut bewährt.

7 VLAN

VLAN steht als Abkürzung für "virtual local area network" und ist im Standard IEEE 802.1q definiert.

Die VLAN-Technologie ermöglicht es, auf einem gemeinsamen physikalischen Übertragungsmedium verschiedene logische Netzwerke parallel zu betreiben, ohne dass es zu einer Kopplung zwischen diesen verschiedenen Netzwerken kommt: Jedes VLAN erhält eine eigene VLAN-ID, und Daten eines VLAN-Teilnehmers werden stets nur an andere Teilnehmer mit der gleichen VLAN-ID weitergeleitet.

Mittels VLAN-Technologie kann daher auch folgendes Problem gelöst werden: Wenn von der NSL oder der AS-POL gleichzeitig Verbindungen zu verschiedenen Schutzobjekten aufgebaut werden, so könnte hieraus eine unerwünschte Netzwerkkopplung zwischen diesen Schutzobjekten entstehen, über die Daten von einem Schutzobjekt in ein anderes gelangen könnten. Dies kann verhindert werden, indem jede Verbindung zu einem Schutzobjekt in einem eigenen VLAN erfolgt: Das EBÜS-Netzwerk-Handbuch enthält konkrete Beispiele, wie so etwas mit Produkten der Firmen Cisco oder Lancom realisiert werden kann.

8 RS232

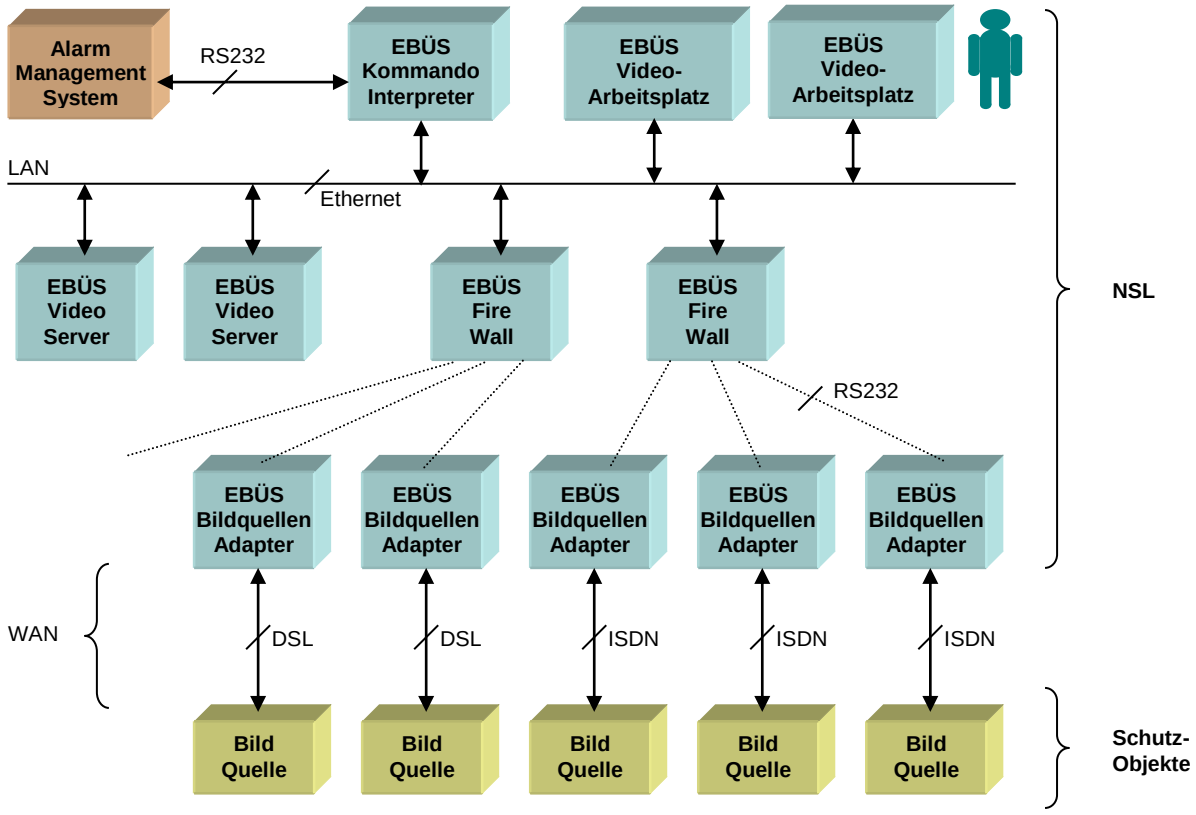
Mit der Abkürzung "RS232" wird die serielle Schnittstelle bezeichnet, die noch aus der Anfangszeit digitaler Datenübertragung stammt und die von vielen Geräten unterstützt wird.

Bisweilen wird argumentiert, nur mit einer "transparenten RS232-Übertragung" könne eine sichere Datenübertragung erreicht werden. Eine RS232-Verbindung ist jedoch nicht per se sicher: Über sie können genau so Viren übertragen werden und Hacker-Angriffe erfolgen wie über jede andere physikalische Verbindung auch.

"Transparent" heißt, dass alle Daten, so wie sie sind, ungeprüft übertragen werden. Sicher wird eine RS232-Verbindung aber erst durch einen Filter auf Empfängerseite, der nur ganz bestimmte, gezielt freigegebene Kommandos und als sicher erwiesene Datenformate passieren lässt, bei allen anderen Datenarten aber Alarm schlägt.

Für EBÜS sind solche RS232-Übertragungsmodule mit integrierter Filterfunktion erhältlich, z.B. um ein EBÜS-System von einem Alarm-Management-System aus zu steuern, ohne dass es zu einer Netzwerk-Kopplung zwischen Videosystem und Alarmsystem kommt.

Auch die Verbindungen zu Bildquellen in den verschiedenen Schutzobjekten können bei EBÜS über solche Filter geführt werden (EBÜS FireWall), um ein Höchstmaß an Sicherheit zu erreichen:



9 HTTPS

HTTP, das "hyper text transfer protocol", wird von Browsern verwendet, um Daten von einem Web-Server abzurufen. Für sicherheitskritische Anwendungen sollte ausschließlich HTTPS verwendet werden. Dies kann gewährleistet werden, indem an der Firewall der Port 80 gesperrt wird, der von HTTP verwendet wird, und stattdessen nur der Port 443 freigegeben wird, über den HTTPS kommuniziert.

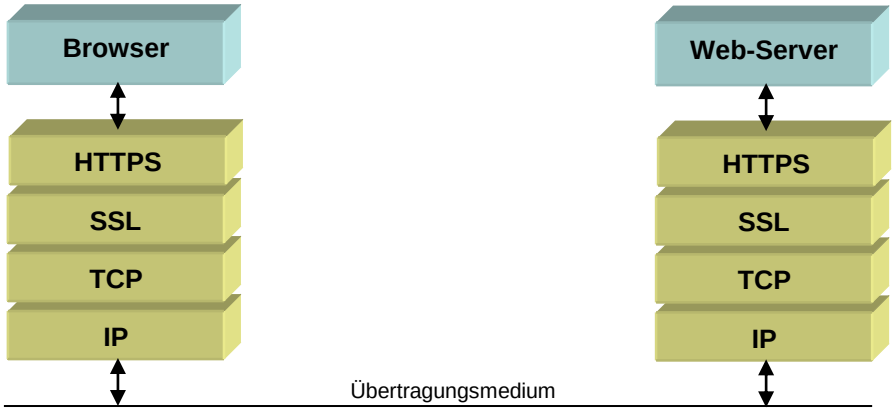
Das "S" steht für "Secure" und beinhaltet eine Reihe von Maßnahmen für einen sicheren Betrieb: Geschützte Identifikation und Authentifizierung der Kommunikationspartner, Verschlüsselung mittels SSL, Verifizierung der Daten mittels Prüfsummen.

Die beteiligten Web-Server (z.B. für den EBÜS-WebExport) müssen entsprechend für einen Betrieb mit HTTPS konfiguriert werden; jeder Zugriff auf den Web-Server sollte selbstverständlich mittels Benutzernamen und Passwort geschützt werden, damit nur berechtigte Nutzer auf die so geschützten Daten zugreifen können.

10 Verschlüsselung

Um die Datensicherheit zu gewährleisten, stehen eine Reihe von Verschlüsselungs-verfahren zur Verfügung, die theoretisch umfassend untersucht wurden und sich praktisch bewährt haben.

SSL (secure socket layer) ist eine Protokollschicht, die im OSI-Schichtenmodell auf IP und TCP aufsetzt und allen darüber liegenden Schichten (z.B. HTTPS) eine gesicherte Kommunikation ermöglicht:



SSL nutzt Verschlüsselungs-Algorithmen wie z.B. AES, IDEA, RSA und Triple DES.
Die aktuelle Weiterentwicklung von SSL heißt TLS (transport layer security).

EBÜS verschlüsselt seine Konfigurationsdaten mit dem SEC-Algorithmus. Dieses Verschlüsselungsverfahren ist im Dokument SEC_Konzept umfassend dokumentiert.

11 Host-Tabelle

In der Host-Tabelle werden alle beteiligten EBÜS-Komponenten mit ihren Namen, IP-Adressen und Dienstarten eingetragen. EBÜS prüft bei jedem versuchten Zugriff auf seine Steuer-Schnittstelle, ob der Anrufer in der Host-Tabelle korrekt registriert ist.

Nur Zugriffe von in der Host-Tabelle registrierten Komponenten werden zugelassen; Zugriffe von unbekannten IP-Adressen werden abgewiesen und führen zu einer Warn-Meldung.

12 IP-Ports

Die IP-Ports, mit denen verschiedene EBÜS-Komponenten miteinander kommunizieren, können vom Administrator frei konfiguriert werden. Somit können die Ports an die jeweiligen Firewall-Einstellungen angepasst werden. Es sollten nur die Ports freigegeben werden, die tatsächlich benötigt werden und deren zugehörige Dienste bekannt sind; alle nicht benötigten Ports sollten gesperrt werden.

13 Passwort

Der Zugriff auf die EBÜS-Steuerschnittstelle ist zusätzlich mit Passwort geschützt. Dieses Passwort kann innerhalb EBÜS nur vom Administrator konfiguriert werden und wird SEC-verschlüsselt gespeichert. Nur bei Anmeldung mit einem gültigen Passwort lässt EBÜS Zugriffe zu.

14 Separate Prozessräume

EBÜS sorgt durch getrennte Prozessräume für jede unter seiner Regie laufende Video-Anwendung dafür, dass es keine Wechselwirkungen zwischen den mit den verschiedenen Schutzobjekten verbundenen Anwendungen gibt.

15 Sicheres Dateisystem

Moderne Dateisysteme bieten auch auf der Ebene des Dateizugriffs zuverlässige Schutzmechanismen vor unberechtigten Zugriffen. Bei Verwendung von Windows sollte daher stets NTFS und nicht mehr das veraltete und unsichere Dateisystem FAT zum Einsatz kommen.

16 Sicherung gegen Fehlbedienung

Das System muss so eingerichtet werden, dass auch bei (absichtlicher oder versehentlicher) Fehlbedienung durch den Anwender die vorstehend beschriebenen Sicherheitsmechanismen nicht umgangen oder außer Kraft gesetzt werden können.

Aktuelle Betriebssysteme bieten dafür das Konzept von Benutzer-Accounts mit eingeschränkten Zugriffsrechten. Jeder Anwender meldet sich beim System mit Benutzernamen und Passwort an und erhält darauf nur die für seinen Aufgabenbereich erforderlichen Zugriffsrechte. Alle sicherheitsrelevanten Einstellungen sind auf diese Weise nur den dafür speziell ausgebildeten und ausgewählten Administratoren zugänglich.

Hierzu zählt beispielsweise, dass die Host-Tabelle mit Administrator-Rechten schreibgeschützt gespeichert wird, damit sie nur vom System-Administrator verändert werden kann. Somit ist es auf Benutzerebene nicht möglich, von anderen als den zugelassenen EBÜS-Komponenten Daten zu empfangen.

Wichtige Dateien wie z.B. Logbücher werden von EBÜS unter dem Systemaccount gespeichert, so dass sie von normalen Anwendern weder gelesen, noch verändert oder gelöscht werden können.

Die Windows-Oberfläche kann vom Administrator so eingerichtet werden, dass der Anwender außer EBÜS keine anderen Anwendungen starten kann, und die Benutzer-verwaltung von EBÜS wiederum stellt dem Anwender gezielt nur die für ihn vorgesehenen Funktionen zur Verfügung.

Um ganz sicher zu gehen, sollten alle sicherheitsrelevanten Geräte in einem abgeschlossenen Raum/Schrank untergebracht werden, so dass auch unberechtigte mechanische Eingriffe in die Sicherheitsmechanismen ausgeschlossen sind.

17 Support / Hotline

Weitere Informationen zu EBÜS finden Sie stets aktuell unter → www.ebues.de

Haben Sie noch Fragen oder Wünsche zu EBÜS?

Dann wenden Sie sich bitte

- telefonisch unter 0511 - 277.2490
- per E-Mail an support@accellence.de

an unsere Hotline. Wir sind Werktags von 9:00-17:00 Uhr zu erreichen.

Wir wünschen Ihnen viel Erfolg bei Ihrer Arbeit mit EBÜS und stehen für Ihre Wünsche und Fragen jederzeit gern zu Ihrer Verfügung.