Mobile Security: Kleine Devices, große Gefahr?

Die Mobile Client – Server Infrastruktur ist Rückgrat der Logistik-Branche, ihre umfassende Absicherung daher Pflicht

Hans Selberdinger ist seit 8 Jahren bei Acteos Experte für IT-Sicherheit. Als Spezialist für Wireless Technologies hat der Informatiker den Status eines Certified Trainers des Acteos-Technologiepartners SOTI, Inc inne. Im Fokus steht hierbei die Lösung MobiControl, die es ermöglicht, mobile Geräte zentral zu überwachen, zu steuern und zu warten.
Mail: hans.selberdinger@acteos.de / Tel.: 08105-385154

1. Ausgangssituation

Mobile Geräte wie PDAs oder Laptops sind heute allgegenwärtig in Unternehmen und über alle Wirtschaftszweige hinweg verbreitet. Das gilt in besonderem Maße für den Logistik-Sektor, in dem Handhelds aus Workflow, Supply Chain und Supply Chain Event Management nicht mehr wegzudenken sind. Sie sind für die Branche Kommunikations- und Geschäftsbasis. Ihr Ausfall oder eine großflächige Beeinträchtigung ihrer Funktionen wirkt sich verheerend aus. Dennoch findet die Sicherheit der übertragenen und empfangenen Daten sowie der Schutz der gespeicherten Informationen auf Handheld oder PDA oft zu wenig Beachtung. Zumal in der Regel moderne Nahbereichsnetze wie Bluetooth, WPAN oder WLAN genutzt werden, die entweder direkt in Man-in-the-Middle-Szenarios angegriffen werden können oder über die Malware vom Mobile Client auf das Netzwerk und umgekehrt übertragen werden kann. Datenzugriff und -synchronisation werden durch spezielle Software gesteuert, die, wenn manipuliert, jederzeit zum Einfallstor für Angriffe werden kann. Als vielleicht gravierendste Sicherheitslücke kann gegenwärtig das mangelnde Risikobewusstsein bei „Mobile Security“ angesehen werden: das vorhandene Sicherheitsmanagement ist in den meisten Firmen unzureichend, um vertrauliche, persönliche oder geschäftskritische Daten zu schützen. Gründe, dies effektiv zu tun, gibt es genug im Hinblick auf Haftung, Compliance, verlorenes Kundenvertrauen, Geschäftsausfälle, Datenspionage und damit Verlust technologischer oder markt-strategischer Alleinstellung.

Generell gilt: Es gibt kein Patentrezept „von der Stange“ für einen umfassenden Schutz. Die Sicherheitspolicy muss, abgestimmt auf die jeweilige IT-Infrastruktur im Unternehmen, vor Ort implementiert werden. Dafür spricht allein schon die große Bandbreite der Betriebssysteme für mobile Endgeräte, die von Windows Mobile über Symbian OS bis hin zu Newton OS, Linux, NetBSD oder OpenBSD reicht. Sicher ist: Schadlogik, sei es in Form von Viren, Spyware,

Keyloggern oder Rootkits, hat die kleinen, tragbaren „PCs“ längst erreicht. Da sich im mobilen Sektor – auch über Note- und Netbook hinaus – bei Smartphone, Black Berry und PDA zunehmend Produkte mit vollwertigen mobilen Betriebssystemen im Einsatz befinden, sind sie in gleicher Weise wie Desktop-PCs durch Trojaner, Intrusion oder Phishing gefährdet. Virenschutz, Firewall, Spyware und (SMS-)Spam-Schutz sind auch bei ihnen das Sicherheitsminimum. Vor allem empfiehlt es sich, sie als Mobile Clients in eine umfassende Client-Server-Sicherheitsarchitektur zu integrieren. Bei all den Gemeinsamkeiten mit den Desktop-PCs gibt es allerdings auch Besonderheiten: Mobile Geräte haben in der Regel diverse Schnittstellen, über die der User Daten lädt. Es gibt eine Vielfalt an Übertragungsverfahren wie WLAN, Bluetooth, GPRS, UMTS und HSDPA – und jede ist ein potenzielles Einfallstor für Hacker. Stationäre Rechner dagegen sind in der Regel nur über das Ethernet mit dem Internet oder Intranet verbunden. Die Sicherheitsmaßnahmen - zudem seit Jahren bewährt und implementiert - können sich bei ihnen daher auf diese Schnittstelle konzentrieren. Des Weiteren sind Desktoprechner leistungsstärker, sodass komplexere Sicherheitssysteme im Hintergrund arbeiten können, ohne den Alltagsbetrieb zu beeinträchtigen. Insbesondere gibt es spezifische Bedrohungsszenarien, die im Sicherheitsmanagement mobiler Endgeräte zu beachten und aus denen ebenso spezifische Gegenmaßnahmen abzuleiten sind.

2.1. Bedrohungsszenario I – Verlust des mobilen Devices

Besonders kritisch ist die Datensicherheit bei Diebstahl und Verlust der Handhelds. Laut Check Point-Statistik (Februar 2008) wurden in Londoner Taxis innerhalb von sechs Monaten 55.000 Mobiltelefone, 5.000 Handhelds, 3.000 Notebooks und 900 USB Sticks liegen gelassen. Leichtsinn mit Folgen. Denn generell gilt: eine fachkundige Person, die unbefugt im Besitz des Gerätes ist, kann jederzeit auf gespeicherte Daten, Adressen, Bilder etc. zugreifen und diese weitergeben. Oder sie kann das Gerät, entweder auf Soft- oder auf Hardwareebene manipuliert, dem Besitzer zurückgeben, noch bevor er den Verlust bemerkt. Durch das Aufspielen von Spyware können dann das mobile Endgerät und ein nach Synchronisation oder Datenaustausch eventuell infiziertes Netzwerk ausgelesen werden.

2.2. Maßnahmen gegen Bedrohungsszenario I

Die Maßnahmen zur Eindämmung dieser Gefahrenquelle zielen zum einen auf Prävention, also Schadensvermeidung, zum anderen auf Schadensbegrenzung, wenn ein Verlust hochsensibler Datenträger eingetreten ist.

2.2.1. Prävention

Die Schulung der Mitarbeiter spielt eine zentrale Rolle. Sie müssen sich ihrer Verantwortung bewusst sein, wenn sie unternehmenskritische Daten mit sich tragen. Aufklärung über Risikoverhalten beim Surfen im oder Downloaden aus dem Internet und über den Umgang mit Firewall und Sicherheitssoftware sollte Inhalt verpflichtender Kurse sein. In ihnen werden

arbeitsrechtlich verbindliche Festlegungen kommuniziert, welche Informationen auf das PDA oder Smartphone gehören und welche Nutzung dieser Geräte eingeschränkt bzw. zugelassen ist. Insgesamt ist es entscheidend, den Umgang mit den Geräten exakt zu definieren. Das gleichzeitige Verwenden eines Gerätes zu privaten und dienstlichen Zwecken sollte strikter Einschränkung unterliegen, das Unbeaufsichtigtlassen oder die Weitergabe der Geräte an Dritte bzw. Fremde unterbleiben. Überflüssige Funktionen, die potenzielle Schwachstellen beherbergen, werden deaktiviert. Idealerweise werden die Daten nicht nur durch ein starkes Password, bestehend aus Buchstaben, Zahlen und Sonderzeichen, geschützt, sondern auch verschlüsselt, sodass sie im Verlustfall des Gerätes nicht ausgelesen werden können.
Firmen- oder Besitzerdaten, die die Identifikation eines verlorenen Endgerätes erleichtern, dürfen nicht auf dem Display oder Gehäuse erscheinen. Insbesondere empfiehlt sich für Unternehmen ein Umdenken: Es muss nicht eigens begründet werden, welche Informationen nach draußen mitgenommen werden. Umgekehrt gehört jede Information, die das geschützte Netzwerk verlässt, auf den Prüfstand. Nur wenn unvermeidlich, darf sie von Mitarbeitern mitgeführt werden. Dabei hat es sich als ratsam erwiesen, eine exakt dokumentierte Zuordnung vorzunehmen, wer welche Information auf welchem Gerät außer Haus trägt. Diese Zuordnung wird am besten ergänzt durch eine Abstufung und Hierarchisierung der mobilen Zugriffsrechte auf das gesamte IT-System. Benutzer und mobile Endgeräte dürfen nur die für ihre Aufgaben (unbedingt) nötigen Rechte innerhalb der Unternehmensinfrastruktur besitzen, sodass der Schaden nach Diebstahl eines PDA oder Smartpohnes begrenzt bzw. das Schadenspotenzial identifiziert und exakt evaluiert werden kann.
Neben solchen Verhaltens- und Organisationsrichtlinien kann auch technisch einiges getan werden, um den Daten- bei Datenträgerverlust präventiv zu minimieren: Dazu gehört beispielsweise die Festlegung der maximalen Speichergröße des mobilen Endgerätes, um massiven Datendiebstahl zu verhindern. Wenn es Gerätehardware und Applikationen erlauben, sollten hoch sensible Daten im mobilen Endgerät auf entfernbaren Datenträgern wie Speicherkarten abgelegt werden. Muss das Gerät aus der Hand gegeben werden (beim Betreten eines fremden Unternehmens), können die unternehmenskritischen Daten sicher mitgenommen werden.

2.2.2. Schadenseindämmung bei eingetretenem Geräteverlust

Remote-Control Systeme, wie MobiControl von SOTI, sind für viele Unternehmen mittlerweile unerlässlich, um Wartung und Monitoring der Geräte on-the-fly vorzunehmen und jederzeit mit den aktuellsten Sicherheitsupdates zu versorgen. Remote Control kann im Notfall die Geräte sogar sperren und auf den Auslieferzustand zurücksetzen. Das schützt vor unbefugter Nutzung oder Servicediebstahl, nicht aber davor, dass der Speicher eines entwendeten Gerätes ausgelesen wird. Wichtig ist, dass das Unternehmen hierfür eine Art Krisenmanagement vorbereitet hat: Zum einen muss der Mitarbeiter einen gravierenden Geräteverlust sofort nach Kenntnisnahme an eine vorher festgelegte Stelle melden. Auch das Festlegen genauer

Zeitfenster für die Geräteverfügbarkeit im Netzwerk sowie das regelmäßige Auslesen der Logfiles sind eine Methode, einen etwaigen Geräteverlust so wie früh wie möglich zu erkennen. Liegt ein solcher Fall vor, muss bekannt sein, welche brisanten Geschäftsinterna von einem Geräteverlust betroffen sind. Dann können Passwörter, Nutzerprofile und Zugangsdaten rechtzeitig geändert werden, bevor das gesamte System kompromittiert wird. Wird das Gerät wiedergefunden und besteht eine gewisse Wahrscheinlichkeit, dass es in fremde Hände gefallen ist, sollte es keineswegs einfach wieder verwendet werden. Eine umfassende Überprüfung auf eingeschleuste Malware, aber auch auf Manipulationen der SIM-Karte ist unerlässlich, bevor es wieder bereinigt und im Auslieferungszustand in Gebrauch kommt. Allerdings: Durch eine hohe Integration der Gerätehardware kann eine weitgehend geschützte, selbst nach Verlust nicht veränderbare Hardware hergestellt werden. Beispiele dafür sind Chipkarten, die auch nach dem Auffinden (fast) nicht unautorisiert benutzt oder verändert werden können.

3.1. Bedrohungsszenario II – Angriff auf das Mobile Endgerät oder seine Kommunikation mit dem Netzwerk

Unsichere Firmennetzzugänge (Internet/WLAN) erlauben Sniffing Attacken oder Man-in-the-Middle Angriffe, bei denen die Kommunikation nicht mehr unmittelbar vom mobilen Endgerät in das Netzwerk führt, sondern über einen Eindringling verläuft, der beiden Kommunikationspartnern das jeweilige Gegenüber vortäuscht. Der Versand von Mails, aber auch die Synchronisierung der Endgeräte kann auf diese Weise ausspioniert werden. Neben solchen direkten Angriffen auf die Kommunikation (wie Abhören, Sniffing, Man-in-the-Middle) besteht darüber hinaus das Risiko einer indirekten Attacke: Hier werden zunächst die Endgeräte mit Malware infiziert, die sich dann im Unternehmensnetzwerk ausbreitet und die Datentransfers Mobile Client – Server manipuliert: über eingeschleuste Keylogger oder SQL-Injektionen werden so Geschäftsinterna Fremden zugänglich gemacht. Die Fremdsteuerung durch Dritte, bei der – analog zu den Botnets bei Desktop-PCs – ein Endgerät zum Versenden von Spam-SMS missbraucht wird, ist ein weiteres Gefahrenszenario.

Hauptmotive solcher Attacken sind entweder Datendiebstahl und Wirtschaftsspionage oder Datenkorruption in der Absicht, das betroffene Unternehmen zu schädigen. Angriffe dieser Art können von außen, aber auch von innen durch unzufriedene Mitarbeiter unternommen werden.

3.2. Maßnahmen gegen Bedrohungsszenario II

Auf der Verhaltens- und Organisationsebene ist es von Vorteil, Regeln für die Installation neuer Software und für den Umgang mit Geräteerweiterungen klar zu definieren und ihre Einhaltung mit technischen oder juristischen Mitteln konsequent durchzusetzen. Neben Richtlinien für den Software-Update Prozesses sind auch Umfang und Freigabe der Erweiterungsslots bei den jeweiligen Endgeräten zu prüfen. Ein Downloaden typischer Risikosoftware wie zip-Files, mp3/mp4–Dateien oder Handygames aus Tauschbörsen oder Social Communities sollte entweder technisch oder durch rechtsverbindliche Absprachen ausgeschlossen werden. Bei den

Nutzern ist die Risiko-Sensibilität zu schärfen, z.B. dafür, mobile Endgeräte ausschließlich mit vertrauenswürdigen Gegenstellen zu synchronisieren und niemals mit unbekannten Geräten. Auf technischer Ebene sind die Endgeräte, zumal wenn sie über ein eigenes, vollwertiges Betriebssystem verfügen, ähnlich zu sichern wie ein Desktop-PC. Virenschutz, Antispyware und Anti-(SMS)-Spam Lösungen sind Pflicht. Autorisierungs- und Schlüsselsysteme für Software-Installationen, wie sie für Chipkarten bzw. JavaCard-Betriebssysteme üblich sind, erhöhen die Sicherheit signifikant.

Der Dialog zwischen Endgerät-Endgerät und Endgerät-Netzwerk kann durch Tunneling oder starke Verschlüsselung effektiv geschützt werden. Sind schon krytopgrafische Verfahren für das gesamte Netzwerk etabliert, sollten PDA oder Smartphone - wie andere Clients auch - in die gesamte Struktur einbezogen werden. VPN-Verfahren, Browser mit SSL/TLS, SSH-Clients und Personal Firewalls kommen hier, je nach benötigtem Sicherheitsgrad und je nach vertretbarem Installations- und Investitionsaufwand, als Lösungen in Frage. Der Einsatz abgesicherter Protokolle wird idealerweise flankiert durch Vergabe starker Passwörter, aber auch durch Benutzerschulung im Handling von Zertifikaten und Sicherheitsschlüsseln. Allerdings sollte nicht allein der Datentransfer verschlüsselt werden, sondern auch lokal gespeicherte Daten (PIN-Manager, E-Mail Encryption). Des Weiteren ist eine effektive Zugangskontrolle bei mobilen Endgeräten unerlässlich: Je nach benötigtem Sicherheitsstandard kommen hier einfache Kennwortabfragen, Schlüsselzuteilung bis hin zur Echtzeithandschrifterkennung auf berührungsempfindlichen Displays zum Einsatz. Darüber hinaus wichtig: Kommunikationsschnittstellen sollten, wenn nicht benötigt, deaktiviert und Logfiles mithilfe von Intrusion Detection Systemen Prüfroutinen unterzogen werden. Dasselbe gilt für Erweiterungsslots, die im Hinblick auf Hardwareerweiterungen am besten regelmäßig kontrolliert, wenn nicht ganz blockiert werden.

4. Sicherheitsmanagement im Unternehmen

Um zu verhindern, dass der Dialog Endgerät-Endgerät bzw. Endgerät-Netzwerk manipuliert wird, müssen Netzwerk und Mobile Clients jeweils für sich selbst gegen Schadlogik, aber auch die zwischen ihnen stattfindenden Datentransfers gegen gezielte Attacken gesichert werden. Es ist von großem Vorteil, hierzu ein zentralisiertes Sicherheitsmanagement mit klar definierten Sicherheitspolicies einzuführen. Dazu gehören die Verwaltung von Sicherheitsprofilen und eine dokumentierte Schlüsselvergabe bzw. -vernichtung, aber auch die Auswertung von Intrusion Detection, Anti-Malware-Programmen und Vulnerability Assessments. Über Remote Control sind von dieser Warte sowohl die Endgeräte (z.B. auf Logfileanomalien) als auch das regelmäßige Updaten und Patchen der Client-/Server-Betriebssysteme bzw. Synchronisationssoftware zu überwachen. Eine IT-Sicherheitspolicy legt dabei fest, welches Verhalten der Mitarbeiter gefordert, erlaubt und verboten ist. Sie legt auch fest, in welchen Abständen Sicherheitsupdates und –checks durchgeführt und welche Gerätefunktionen für welchen Personenkreis freigegeben werden, welche nicht. Ihr liegt eine Analyse zugrunde, die sich an

der benötigten Leistung des Systems und an den damit verbundenen Risiken orientiert. Eine Policy sollte stets an die Einsatzumgebung angepasst werden: Sie darf nicht zu strikt sein, also wertvolle IT-/Telco-Funktionalitäten aufgrund überschätzter Risiken unterdrücken; sie sollte allerdings auch nicht zu viele Freiheitsgrade lassen, die Angreifern Tür und Tor öffnen. Die konkrete Umsetzung beginnt mit einer Analyse des Ist-Zustandes: Welche Geräteklasse bzw. welcher Gerätetyp ist im Einsatz? Welche Dienste sind aktiviert? Welche Sicherheitsdirektiven sind bereits für das Netzwerk bzw. die mobilen Clients implementiert? Welche Anforderungen an das System bestehen? Danach wird eine Risikobewertung vorgenommen und ermittelt, wo Schwachstellen liegen, wie sie beseitigt werden können und ob hierfür der (finanzielle, personelle und organisatorische) Aufwand vertretbar ist. An dieser Stelle spielt eine entscheidende Rolle, wer als Gefährder angesehen wird: Betrüger von außen oder leichtsinnige, vielleicht sogar kriminelle Insider. Auch wichtig: Welche Szenarien sind wahrscheinlich? – Betrug, Diebstahl oder Datenvandalismus frustrierter Mitarbeiter? Schließlich ist zu evaluieren, ob das Risiko und seine Gegenmaßnahmen eine bestimmte Einschränkung der Telco-Funktionalitäten rechtfertigen. Im letzten Schritt wird der Soll-Zustand der IT-Sicherheit definiert. IT/Telco-Sicherheitsrichtlinien legen z.B. die Frequenz zentralisierter Passwort- und automatischer Integrationsprüfungen der mobilen Geräte und der Infrastruktur fest. Hierbei stehen alle vier Phasen im Lebenszyklus der Mobilen Clients gleichermaßen im Fokus: Beschaffung, Installation, Betrieb und Außerdienststellung. Nicht vergessen werden darf, Fristen sowie geeignete Kontrollmechanismen und Verantwortlichkeiten festzuschreiben, die sicherstellen, dass die Policy auch umgesetzt wird.

5. Beispiel für einen Lösungsansatz aus der Praxis

Gestützt auf langjährige Erfahrungen bei Field-Service-Lösungen, mobiler Datenerfassung und -verarbeitung hat Acteos ein umfassendes Sicherheitskonzept entwickelt. Zu ihm zählen Schulungen, Consultings und eine partnerschaftliche Projektunterstützung bei der Implementierung von IT- und Telco-Security Standards.

Auf technologischer Ebene basiert das Acteos Sicherheitspaket auf einer Online IP-VPN Lösung in Kooperation mit Telefonprovidern. Mit der Einrichtung einer geschlossenen Benutzergruppe stellt dieser hierbei sicher, dass nur berechtigte Mitarbeiter mit autorisierten Karten auf das Intranet zugreifen können. Über einen gesicherten VPN-Tunnel wird die IP-Verbindung zwischen dem Unternehmens- und dem Providernetz aufgebaut. Ein VPN-Client auf dem Endgerät ist nicht erforderlich. Entscheidend bei diesem Konzept ist es, dass die Firmen- und Provider-Gateways miteinander durch ein Virtual Private Network (VPN) vor Fremdzugriff geschützt sind. Ergänzt wird dieses Grundgerüst sicherer Kommunikation durch Gerätemanagement-Funktionalitäten. So kann im Rahmen gestufter Sperrungen der Zugriff auf die Gerätesteuerung für den Mitarbeiter eingeschränkt werden, sodass eine fehlerhafte Installation von Software sowie die ungewollte Implementierung von Schadlogik weitestgehend ausgeschlossen und Ausfälle oder sogar Infektionen des Netzwerks über die Synchronisation vermieden werden. Das

„Advanced Security“ Paket von Acteos sieht darüber hinaus Ablaufüberwachungsverfahren für Anwendungen vor: Direkt in das Betriebssystem integrierte Sicherheitslösungen verhindern, dass zugangsbeschränkte Anwendungen auf mobilen Geräten unterstützt werden oder Fremdsoftware, im schlimmsten Fall Malware, auf dem Gerät lauffähig ist. Weiterhin erlauben spezielle Steuerungsverfahren, die Hardwarefunktionen der Geräte selektiv zu deaktivieren. Gemäß individueller Nutzer-, Abteilungs- oder Niederlassungsprofile können Bluetooth- und Infrarot-Anschlüsse oder Hardwarefunktionen wie USB-Schnittstellen blockiert werden, um den unerlaubten Download von Daten durch eigene Mitarbeiter zu unterbinden. Darüber hinaus bietet Acteos seinen Kunden als autorisierter Partner die Hardware-Management Lösung MobiControl der kanadischen Firma SOTI, Inc. an. Als Dienstleister übernimmt Acteos auch die Einrichtung dieses Remote Control Systems. Mit ihm werden im Einsatz befindliche Geräte zentral und on-the-fly mit Sicherheitsupdates versorgt und – falls gestohlen, verloren oder innerhalb eines bestimmten Zeitintervalls kontaktlos - offline geschaltet, um einem Missbrauch des betroffenen Mobile Client effektiv entgegenzutreten.

6. Fazit

Kleine Devices, große Gefahr? - Mobile Endgeräte sind heute zunehmend mit vollwertigen Betriebssystemen ausgestattet. Das erhöht ihre Funktionalität, macht sie bei Optimierung von Workflow oder Supply Chain Management unverzichtbar – aber gleichzeitig auch angreifbar. Wer allerdings auf eine Sensibilisierung der Mitarbeiter für Risiken achtet und das Implementieren eines umfassenden Sicherheitskonzepts nicht vernachlässigt, für dessen IT- und Telco-Infrastruktur gilt: Kleine Devices, großer Nutzen. Mit Sicherheit.

Glossar

Botnet	Missbräuchliche Zusammenschaltung infizierter Rechner zu einem illegalen Netzwerk: Durch Einschleusung von Schadsoftware kann ein Unbefugter die Kontrolle über gekaperte PCs und Server übernehmen, um deren gesamte Rechenleistung z.B. zu Spamversand oder Internetsabotage gebündelt einzusetzen.
Keylogger	Software, die Eingaben (Passwörter, PIN) über die Tastatur protokolliert und diese Informationen u.U. Datendieben zur Verfügung stellt.
Man-in-the-Middle	Angriffsszenario, bei dem der Angreifer den Kommunikationspartnern das jeweilige Gegenüber vortäuschen kann, ohne dass sie es merken. Statt direkt von A nach B läuft der Datentransfer über den Eindringling, der so Spionage oder Datenmanipulation betreiben kann.
Online IP-VPN	Die im Internet-Protokoll (IP) formatierten Daten werden bei ihrer Übertragung so verschlüsselt, dass die Kommunikation weder abgefangen noch abgehört werden kann.
Remote Control	Fernwartung und -überwachung von Geräten in der IT.
Rootkit	Software, die das Kapern von Rechnern durch einen unbefugten Dritten verschleiert.
Sniffing-Attacke	Datendiebstahl mithilfe einer Schadsoftware, die netzwerkinterne Datentransfers „erschnüffeln“, also empfangen, aufzeichnen, darstellen und auswerten kann.
SQL-Injektionen	Einschleusung illegaler Befehle über eine Sicherheitslücke in der Zugangssoftware zu einer Datenbank: Ziel ist es zumeist, den Datenbestand (TAN, PIN, Passwörter) auszulesen.
SSH	Secure Shell: Netzwerkprotokoll, das eine sichere, verschlüsselte Daten- und Dateiübertragung ermöglicht, z.B. über HTTPS.
SSL	Secure Sockets Layer: Verschlüsselungsprotokoll zur Daten- und Dateiübertragung über das Internet.
TLS	Transport Layer Security (TLS) cf. SSL
Tunneling	Verfahren zum Aufbau abhörsicherer Verbindungen über ungesicherte Computernetzwerke hinweg. Dadurch wird eine verschlüsselte Datenübertragung auch für Dienste realisiert, die über keine eigenen Verschlüsselungsverfahren verfügen.
VPN	Virtual Private Network: Verfahren, das mithilfe der Tunneling-Technologie eine gesicherte Übertragung sensibler Daten über ein öffentliches Netzwerk (Internet) gewährleistet.
Vulnerability Assessment	Präventives Aufspüren und Bewerten von Schwachstellen, über die sich IT-Kriminelle Zugang zu einem Netzwerk, Server oder PC verschaffen können.