

# Sicherheit im Intranet

## 1. MANAGEMENT SUMMARY

Dieses Whitepaper setzt sich mit der heute immer noch vorhandenen Schwachstelle auseinander, dass Daten im Intranet unzureichend geschützt sind. Die wenigsten Unternehmen denken darüber nach, wie sie nicht nur den Zugriff auf die Daten absichern sondern auch den Transport über die Netzwerke sicher und gegen die häufigsten Attacken schützen können.

Seit vielen Jahren setzt sich das Bundesdatenschutzgesetz, neben einer Reihe von anderen Gesetzen und Verordnungen mit der Speicherung von Daten auseinander. Leider fehlt in allen derzeit aktuellen Gesetzen, Verordnungen und Richtlinien die Auseinandersetzung mit dem Thema des Datentransports. Im Falle eines physikalischen Transports von Daten in Form von Speichermedien wird darauf geachtet, dass diese sicher von einem Ort zum anderen gelangen. Werden die Daten jedoch elektronisch bewegt, also in Form von Netzwerktransport, so wird nur dann auf Sicherheit geachtet, wenn die Daten das Unternehmen verlassen. Solange die Daten im internen Netz des Unternehmens bewegt werden reicht es den Verantwortlichen offenbar, wenn sie nicht aus Versehen das Unternehmen verlassen. Ganz wenige Unternehmen denken darüber nach wie auch der interne Datentransport, also die Intranet-Umgebung, geschützt werden kann. Von diesen Unternehmen wiederum setzen noch weniger die heute verfügbaren Methoden ein, um tatsächlich gegen Angriffe von innen geschützt zu sein.

Dieses Whitepaper soll dazu dienen die Verantwortlichen für dieses Thema zu sensibilisieren, ihre Netzwerkstruktur zu analysieren und notwendige Maßnahmen zu realisieren. Es kann und darf nicht damit getan sein, einen Safe zu besitzen, um Daten zu speichern. Es muss auch dafür gesorgt werden, dass der Firmenwagen für den Transport der Daten gesichert und geschützt ist, damit keiner die sensiblen Daten stiehlt und damit die Verantwortlichen vor große Probleme stellt.

Das Kernthema für dieses Papier ist im Bereich der Terminal-Emulatoren angesiedelt. Jedoch sind diese Bereiche auch auf andere Sektoren der Netzwerktechnologie übertragbar. Angriffssimulationen und Analysen zeigen Schwachstellen im inneren Netz eines Unternehmens schnell auf und geben Rückschlüsse auf die Verhinderung von solchen Attacken.

Handeln Sie verantwortlich und analysieren Sie Ihre internen Strukturen. Widerstand gegen Technologien haben keine Grundlage. Über 70% der Datendiebstähle werden von Mitarbeitern begangen. Das sollte zum Nachdenken alleine genügen. Nach der Lektüre dieses Whitepapers haben Sie die notwendigen Methoden an der Hand, um diese Zahl möglichst bereits morgen zu reduzieren.

## **2. DIE SICHERHEIT BEI DER DATENSPEICHERUNG**

Als ich vor mehr als zwanzig Jahren in der Datenverarbeitung angefangen habe, war es noch üblich, dass während der Gehaltsabrechnung die zuständige Person im Rechenzentrum darüber wachte, dass die Abrechnungen nicht vom Operating gelesen werden. So wurden abstruse Vorgänge wie ein schwarzes Tuch über dem Drucker oder andere abwegige Verhalten an den Tag gelegt. Nie werde ich vergessen, welchen Schock unsere Lohnbuchhalterin eines Tages bekam, als sie wieder einmal über dem Drucker wachte als die Abrechnung gedruckt wurde. Hinter ihrem Rücken rief der Operator das Spool-Display Programm auf, um die Daten anzusehen. Natürlich fragte er sie dann etwas irritiert, warum sie mit dem Gehalt denn jetzt Operating spielt. Unsere Lohnbuchhalterin wurde leichenblass und verlangte sofort, dass dieses Programm stillgelegt wird. Seit diesem Tag war mir klar, dass Sicherheit nicht damit beginnt, die gedruckten Informationen zu schützen. Jedes Unternehmen setzt heute dazu ACL's (Access Control Lists) oder ähnliche Verfahren ein, um sicherzustellen, dass nur berechtigte Personen auf die Daten zugreifen dürfen. In Banken, Versicherungen und öffentlichen Behörden wachen Revisoren darüber, dass diese Regelwerke eingehalten werden und „wasserdicht“ sind. Personenbezogene Daten besitzen sogar ein eigenes Gesetz, damit kein Unternehmen diese Daten ungeschützt behandelt. Der Personenkreis der mit diesen Daten umgeht muss entsprechend dem Gesetz eingewiesen und auf dieses Gesetz vergattert sein.

## **3. UND WAS IST MIT DEM TRANSPORT ?**

Ein wenig leichtgläubig ist man in der Vergangenheit mit dem Datentransport umgegangen. Selbst heute findet man immer noch Unternehmen, die Daten außerhalb der internen Netzwerke unverschlüsselt transportieren. Das entspricht dem Taxi, das man mit dem Transport von Listen beauftragt in denen die Gehälter offen liegen. Solches Vorgehen ist nicht nur leichtsinnig sondern bereits grob fahrlässig. Gleich verhält sich jeder, der mit einer Kreditkarte bezahlt und den Beleg unachtsam wegwirft. Auf diesen Belegen finden sich alle notwendigen Informationen, um im Internet einzukaufen. Kartenummer, Name, Gültigkeitsdauer. Mehr ist heute nicht notwendig, um Schaden zu verursachen. Besitzer von Kreditkarten wundern sich dann und sprechen von der Unsicherheit bei Kreditkarten. Es ist nicht die Kreditkarte die unsicher ist, sondern der Besitzer der diese Informationen nicht schützt.

Nun sind jedoch Banken, Versicherungen und die öffentlichen Behörden soweit sensibilisiert, dass sie darauf achten Informationen im Internet, wenn sie denn persönlichen Charakter besitzen, mittels SSL zu verschlüsseln. Mit dieser Sicherheit wird auch gerne auf den Internetseiten dieser Anbieter geworben. Sie vermitteln dem Anwender, dem Client, das Gefühl von Sicherheit das ihm auch zusteht. Sicher gibt es immer wieder Angriffe, die versuchen auch diese Sicherheit außer Kraft zu setzen, jedoch sind diese Angriffe rar und nur von Profis real durchzuführen.

Was geschieht aber nun mit den Daten, nachdem sie verschlüsselt und gesichert auf dem Server des Unternehmens gelandet sind?

Sie werden von dort über Firewalls ins Innere transportiert und dort weiter verarbeitet.

Wie werden sie transportiert?

In den meisten Fällen unverschlüsselt und ungesichert!

Warum das so ist weiß eigentlich keiner so genau. Es ist meistens die Unwissenheit der zuständigen Entwickler, dass Verfahren eingesetzt werden die lediglich die Anwendungslogik der Werkzeuge und Datenbanken kennen. Selten hat ein Entwickler gesehen, wie die Daten transportiert werden. Ebenso selten hat ein Revisor danach gefragt.

Nun landen die Daten des Kunden auf dem Rechner bei einer Bank, einer Versicherung oder einer öffentlichen Behörde. Da die Mehrzahl dieser Unternehmen als Plattform für die unternehmenskritischen Anwendungen den Mainframe einsetzt, sind dies IMS/CICS Transaktionen gegen DB2, Oracle oder andere Datenbanken.

Nun wird ein Mitarbeiter dieses Unternehmens mit seinem „Terminal“ diese Daten ansehen und verarbeiten. Das Terminal ist eigentlich keins mehr. Heute werden PC's für diese Arbeit eingesetzt. Die Programme die diese Funktion erfüllen nennen sich Terminal Emulatoren. Früher waren diese Emulatoren als Ersatz für die Terminals eingeführt worden und besaßen noch eigene „Emulator-Karten“. Vorreiter auf diesem Gebiet waren die Irma-Karte von DCA und die PC3270-Karte von IBM. Eine Vielzahl anderer Hersteller hat sich diesem Markt angeschlossen. Die größten heißen NetManage, Attachmate, IBM und OpenConnect Systems. Letzterer ist zwar nicht in jedem Unternehmen bekannt, jedoch in den Bereichen in denen Sicherheit eine Rolle spielt bestens eingeführt.

Als nun die Einführung der TCP/IP Netze in den Unternehmen nach und nach andere Netzwerke verdrängte, wurden auch die Emulatoren flexibler. Im Jahre 1982 wurde das erste SNA-TCP/IP Gateway von OpenConnect Systems angeboten. Also ein System, dass diese Netze miteinander verbindet und Dienste bereitstellt, die eine Terminalemulation auch in TCP/IP ermöglicht. Seit diesem Zeitpunkt wurden immer mehr der Terminal-Emulatoren mit der Funktionalität für TN3270 ausgestattet. Zwischenzeitlich ist es bereits „normal“, dass man über TN3270/TN3270E auf den Mainframe zugreift, da die Gateways entweder direkt auf dem Mainframe genutzt werden oder über die CISCO Router implementiert sind. Neben diesen, am häufigsten eingesetzten Mainframe Gateways, werden auch andere Hersteller verwendet so auch nach wie vor das OpenConnect SNA Access Server Gateway.

Dieser „schleichende“ Übergang von einer Punkt-zu-Punkt Verbindung, die durch SNA (System Network Architecture – also die Netzwerkarchitektur des Mainframes) sichergestellt war zu einer Multi-Punkt Verbindung, wie es TCP/IP realisiert hat wohl dazu geführt, dass man es schlichtweg vergessen hat, darüber nachzudenken wie diese Kommunikation geschützt werden kann.

Anders ist es nicht zu erklären, warum der Transport der TN3270 Datenströme immer noch ungeschützt erfolgt. Es ist trivial und einfach die Datenpakete, die Client und Server miteinander austauschen, mitzulesen. Es kommt der eingangs beschriebenen Situation der Lohnbuchhalterin schon sehr nahe, wenn jeder die Speicherung schützt, nicht aber den Transport. Datenmonitore wie Ethereal, Sniffer oder MS NetworkMonitor sind heute in der Regel leicht zu erhalten. Insbesondere Ethereal ist als Freeware Paket für Administratoren eine beliebte Lösung und im Internet unter [www.ethereal.com](http://www.ethereal.com) für jeden herunter zu laden. Von dort bis zum Mitlesen der Daten ist der Weg nun wahrhaftig nicht mehr weit. Frustrierte

Mitarbeiter, innere Kündigungen oder kriminell veranlagte Kollegen können nun schalten und walten.

## 4. SICHERHEIT ABER WIE ?

Wie können Sie diese Angriffe, die immerhin zu ca. 70% von Mitarbeitern durchgeführt werden, abwenden?

Zunächst sollten zwei verschiedene Probleme betrachtet werden. Hierbei wird sich in diesem Papier auf die Terminal-Emulatoren konzentriert.

Viele Anbieter unterstützen eine Verschlüsselung der Daten. Generell ist es bis heute nicht üblich, die TN3270 Dienste zu verschlüsseln. Deshalb wird vielfach ein weiteres Gateway eingesetzt. Das ist zunächst eigentlich nichts schlimmes. Schwierig wird es, wenn dieses Gateway und der Emulator lediglich verschlüsseln. Warum, werden sich viele fragen. Weil die Verschlüsselung lediglich einen Teil der Problematik behandelt. Oftmals findet sich Software im Einsatz, die Verschlüsselung als Sicherheitskriterium hervorhebt. Es hört sich halt gut an, wenn von einer 128-Bit Verschlüsselung gesprochen wird. Verantwortliche neigen dazu, dies in einen Topf mit SSL und 128-Bit zu werfen. Dieser Fehler ist fatal und leichtsinnig. Es entspricht einem PKW der zwar den Airbag, nicht aber die Sensoren für die Auslösung besitzt. Jede Verschlüsselung ist so gut wie die Methode die es verwendet. Anbieter auf dem Markt verwenden Verschlüsselungen, die als OpenSource im Internet bereit stehen und somit von jedem gewieften Techie verwendet werden können.

Es kommt nämlich noch ein zweites Problem hinzu. Angriffsszenarien sprechen oftmals von der Man-in-the-Middle Attacke. Was darunter zu verstehen ist lässt sich relativ leicht erklären.

Ein Client (Anwender) verbindet sich via TCP/IP mit einem Server. Dieser Server wird über eine IP-Adresse angesprochen. Es ist bekannt, dass es Menschen schwer haben mit Nummern umzugehen. Deshalb gibt es im TCP/IP die Namensauflösung. Wer weiß schon, dass sich hinter der IP-Adresse 195.125.196.194 der Name www.sagadc.de befindet. Der Benutzer verwendet fast immer den Namen des Servers (also hier www.sagadc.de). Dieser Name wird durch den DNS (Domain Name Server) aufgelöst und als 195.125.196.194 von dem Programm angesprochen. Nun ist das Dilemma, dass DNS oftmals Ziel von Angriffen sind. So wurden im Jahr 2002 die zentralen DNS eines großen ISP (Internet Service Provider) angegriffen und verändert was dazu geführt hat, dass jeder Benutzer dieses ISP nicht die gewünschte Seite im Browser erhielt sondern an eine politisch angehauchte Seite umgeleitet wurde.

In einem internen Netz gibt es ebenfalls DNS die für die Umsetzung intern verwendet werden. Auch diese sind angreifbar und mit geringem Aufwand modifizierbar. Ebenso ist es möglich die lokale Namensauflösung (hosts-Datei) auf den PCs zu modifizieren. Nun verbindet sich ein Anwender nicht mehr gegen den TN3270 Server sondern gegen einen Server der als „Proxy“ fungiert. Dieser nimmt die Daten entgegen und leitet sie an den ursprünglich gewünschten Server weiter. Diese Daten können „natürlich“ gelesen, gespeichert und modifiziert werden. Von diesen Vorgängen erfährt der Benutzer gar nichts. Sind diese Daten verschlüsselt hat der „Angreifer“ nun genügend Zeit sich mit der Entschlüsselung auseinander zu setzen. Da es sich in den meisten Fällen um OpenSource handelt, dauert es nicht lange bis

dies gelingt. Eine Analyse bei SAGA D.C. hat gezeigt, dass ein Anwendungsentwickler ca. 2 Stunden für die Entschlüsselungslogik brauchte. Also ist Verschlüsseln nicht alles. Es muss sichergestellt sein, dass der Server der kontaktiert wird auch tatsächlich derjenige ist, den man erwartet. Hier kommt nun das Konzept von SSL zum Tragen. SSL oder die neuere Variante TLS (SSL = Secured Socket Layer, TLS = Transport Layer Security) setzt neben der Verschlüsselung noch Zertifikate ein, die einem Server zugewiesen sind. Nur wenn alle Informationen des Zertifikates stimmen, ist eine sichere Verbindung möglich. Aus diesem Grund sind diese Verfahren im Internet im Einsatz und bieten einen hohen Sicherheitsstandard. Das Gleiche gilt auch für das Intranet.

Einziges Manko bei diesem Konzept ist, dass die wenigsten Anbieter von Emulatoren SSL bzw. TLS zur Verschlüsselung anbieten und die wenigsten Gateways SSL für den TN3270 Dienst (TN3270S) bereitstellen. Somit ist es notwendig die wenigen Anbieter dieser Komponenten zu analysieren und deren Stärken und Schwächen miteinander zu vergleichen. Gerade bei den heute mehr und mehr zum Einsatz kommenden Java-basierten Clients (Emulatoren) ist die Anzahl der Anbieter stark eingeschränkt.

## **5. WELCHE TECHNIKEN GIBT ES?**

Ausgehend von Java-basierten Clients werden in der Regel Gateways (Three Tier Solutions) angeboten. Ein Produkt wie OC://WebConnect Pro ist innerhalb von 15 Minuten installiert und in der Lage zwischen dem Client und dem OC://WebConnect PRO Server SSL zu verwenden. Daneben ist die Frage, ob zwischen dem OC://WebConnect PRO Server und dem TN3270 Server ebenfalls SSL verwendet werden soll. Beide Strecken sind mit Hilfe von SSL abzusichern und je nach Installation konfigurierbar. Der Client entspricht einem „Full-Featured Fat Client“, also dem bisher bekannten 3270 Emulator mit all seinen Funktionen. Daneben besteht auch noch die Möglichkeit über Programmierschnittstellen in JAVA Applikationen zu erstellen, die jede erdenkliche Oberflächenveredelung ermöglicht.

Bei diesem Produkt hat sich als entscheidender Vorteil herausgestellt, dass es über eine HTTPS-Strecke (also eine HTTP-SSL Strecke) auch die Verbindung zum Gateway tunnelt (verbirgt). Dadurch wird nur ein Port im internen Firewall benötigt was wiederum ein verbessertes Maß an Sicherheit darstellt. Dieses Verfahren ist patentiert und als Differenzierungsmerkmal anzuerkennen.

Das Gateway OC://WebConnect PRO ist skalierbar von kleinen Installationen (Windows 2000) bis zu Installationen für Linux z/Series (also der Mainframe Umgebung). Die Administration erfolgt ebenso zentral wie die Verteilung von neuen Versionen. Es wird keine Software Distribution benötigt, da JAVA bereits diese Funktionalität beinhaltet. Die größte derzeit in Europa betriebene Installation von OC://WebConnect PRO befindet sich bei einer der größten Banken in Europa in Schottland und bietet 60.000 Benutzern einen gesicherten Zugriff auf die Daten des Mainframes.

## **6. UND WAS IST MIT ANDEREN DIENSTEN ?**

Natürlich gibt es eine Reihe von Diensten und Protokollen, die bisher unverschlüsselt bereitgestellt werden. Die größte Schwäche bieten derzeit die UNIX-Systeme die mit dem Protokoll Telnet bzw. rlogin arbeiten. Ein Tool zur Analyse von Schwachstellen ist NNESSUS. Unter [www.nessus.org](http://www.nessus.org) können weitere Informationen hierzu nachgelesen werden und die Software (Freeware) herunter geladen werden. Nessus verwendet die bekanntesten Angriffsszenarien und wird am besten gegen alle Systeme eines Netzes gefahren. Dabei ergibt sich eine Inventarliste mit Schwachstellen die in eine Datenbank gestellt werden kann. Anschließend kann man monatlich Abweichungen von dieser „ursprünglichen“ Analyse fahren, um festzustellen ob irgendwelche neuen Schwachstellen aufgedeckt wurden oder sich jemand an den Systemen zu schaffen gemacht hat. Nessus verwendet Script-Files die auch selbst für eigene Angriffsszenarien erstellt werden können. Daneben werden Hinweise für Alternativen aufgezeigt.

Sicherlich kann nicht jede Schwachstelle beseitigt werden, es sollte jedoch die Hürde für das Eindringen in ein System so hoch wie möglich gelegt werden. Außerdem kann bei zukünftigen Entscheidungen für neue Systeme, sei es Anwendungen oder Systemkomponenten, darauf geachtet werden ob die Sicherheitsaspekte die bislang als Schwachstelle oder Angriffspunkt bekannt sind, mit der neuen Entscheidung beseitigt sind. Nur über den Druck der Anwender (Kunden) werden durch die Hersteller Sicherheitsmechanismen umgesetzt und integriert.

Verschlüsselung, Server-Authentifizierung und das Schließen aller nicht notwendigen Ports auf UNIX Systemen verringert die Möglichkeit von Angriffen dramatisch. Daneben sind natürlich Firewalls auch für die internen Netze unabdingbar.

## **7. ZUSAMMENFASSUNG**

Aus heutiger Sicht bietet das Intranet immer noch genügend Angriffsfläche für den Datendiebstahl oder die Datenmanipulation. Ca. 70% aller Angriffe und Datendiebstähle werden aus dem Unternehmen heraus ausgeführt. Die Verluste die diese Angriffe verursachen gehen in die Milliarden und schädigen die Unternehmen und die Urheber dieser Daten, oftmals Kunden und Lieferanten.

Eine wesentliche Schwachstelle bei diesen Betrachtungen ist die Art die Terminal-Emulation für den Mainframe. Seit der Einführung von TCP/IP als Protokoll wurde seitens der meisten Unternehmen vergessen, auf die Sicherheit der Mainframe Zugänge zu achten. Bei einer Analyse einer großen Schweizer Bank im Jahre 1995 hat man festgestellt, dass man maximal 14 Tage benötigt, um die Userids und Passwörter aller 17.000 Benutzer zu ermitteln. Das dies ohne großen Aufwand möglich ist liegt an der fehlenden Sicherheit auf der Transportebene dieser Daten. Die Informationen werden unverschlüsselt übertragen und bieten somit jedem Angreifer ein einfaches Ziel für Diebstähle, Manipulationen oder Attacken.

Obwohl seit 1997 für diese Emulatoren von OpenConnect Systems die SSL Verschlüsselung angeboten wird, sehen Sicherheitsbeauftragte, Revisoren und CIO/CTO gerne weg wenn es um dieses Thema geht.

OC://WebConnect PRO als Java basierte Client und OC://WebConnect SNA Access Server als SNA-TCP/IP Gateway bieten SSL Verschlüsselung auf der gesamten Strecke zwischen Client und dem Mainframe.

Verschlüsselung alleine bietet nicht die Sicherheit, die mit SSL bzw. der neueren Variante TLS garantiert wird. Nur SSL/TLS bietet neben einer hohen Verschlüsselungssicherheit auch die Authentizität des Servers mit dem sich der Anwender verbindet. Die gleichen Maßstäbe die im Internet angelegt werden sollten auch für die Internen Netze (Intranets) gelten. Verantwortliche im Bereich Sicherheit und Revision sind aufgefordert, das Thema der Datensicherheit nicht nur für die Datenspeicherung und den Zugang hierzu, sondern auch für den Transport der Daten über die Netzwerke zu betrachten. Nur dann ist gewährleistet, dass Daten von Kunden, Lieferanten und Mitarbeitern nicht in die falschen Hände geraten und dem Unternehmen hierdurch Schaden in beträchtlicher Höhe entsteht.

Die Produkte sind auf dem Markt verfügbar. Es ist nur notwendig sich mit diesem Thema auseinander zu setzen und die Umsetzung dieses wichtigen Bereichs schnellstens anzugehen.