



SICHERHEITSRISIKEN BEIM NETZWERKDRUCK

Lösungen vom PC bis zum fertigen Ausdruck

In jedem Unternehmen und in jeder Organisation gibt es vertrauliche Daten und Dokumente, die vor unberechtigtem Zugriff geschützt werden müssen. In der IT-Abteilung sorgen Sicherheitsmaßnahmen wie Passwortqualität, SSL/TLS- oder VPN-Verbindungen für die Sicherheit sensibler oder unternehmenskritischer Daten. Aufgrund bestehender Datenschutzgesetze sind Institutionen und Unternehmen zudem verpflichtet, personenbezogene Daten vor unberechtigtem Zugriff zu schützen. Die Erkenntnis, dass zu einem konsequenten Sicherheitskonzept auch das sichere Drucken im Netz gehört, setzt sich immer stärker durch. Die eingangs erwähnten Sicherheitsmaßnahmen sind nämlich unter Umständen vergeblich, wenn sensible Druckdaten praktisch im Klartext durch das Netz geschickt werden. Dieses White Paper beleuchtet die Sicherheitsrisiken, denen ein Druckjob auf seinem Weg von der Workstation des Anwenders bis zur Ausgabe am Drucker begegnet und stellt Lösungen vor.

THORSTEN KILIAN

Produkt Manager

MARGARETE KEULEN

Marketing Communications Manager

Version 1.0

November 2006

INHALTSVERZEICHNIS

1. SICHERHEITSRISIKEN BEIM NETZWERKDRUCK	3
2. DER DRUCKJOB IM NETZ: IM Dschungel DER SICHERHEITSRISIKEN	4
2.1. Sicherung von Daten, Workstations und Applikationen	4
2.2. Zugang zum Netz – mit oder ohne Kontrolle	4
2.3. Vom Netzwerktyp bedingte Sicherheitsrisiken	6
2.4. Netz-Subsystem – Sicherheit durch Netzwerkkomponenten	7
2.5. Netzwerkprotokolle mit integrierten Sicherheitsmechanismen	7
2.6. Druckdatenverschlüsselung mit SSL/TLS	7
2.7. Zugriffsrechte auf das Output-Gerät	8
2.8. Ausgabe des Druckdokuments am Drucker an berechnigte Anwender	9
3. SEH-LÖSUNGEN FÜR SICHERES DRUCKEN IM ÜBERBLICK	10
3.1 SEH Printserver für bestimmte Netzwerkmedien	10
3.2 Benutzer-Authentifizierung	10
3.3 Zugriffs- und Konfigurationsschutz der SEH Printserver	11
3.4 Zugriffsschutz auf Drucker	11
3.5 Druckdatenverschlüsselung mit SSL/TLS (128 Bit-Verschlüsselung)	12
3.6 Follow Me Printing-Lösung mit SEH Printserver	12
4. SICHERE NETZWERK-DRUCKLÖSUNGEN VON SEH AUF EINEN BLICK	13
5. LITERATUR	14
6. INTERNET	14

1. SICHERHEITSRISIKEN BEIM NETZWERKDRUCK

Sicherheit definiert der VDI-Ausschuss „Technik – Risiko – Kommunikation“ als „einen Zustand, in dem das verbleibende Risiko als akzeptabel eingestuft wird.“ Und er fügt hinzu: „Es besteht also auch bei Sicherheit noch die Möglichkeit, dass ein Schaden eintreten kann.“¹ Sicherheit ist also nie absolut, sondern immer relativ. Daher ist es sinnvoll, Sicherheitsrisiken abzuschätzen und festzulegen, was im jeweiligen Fall als Sicherheitsrisiko definiert wird, wie dieses Risiko zu bewerten ist und wie es sich minimieren oder ausschalten lässt.² Bei einer Auditierung zu IT-Sicherheit unterscheidet man gewöhnlich zwischen Kompromittierung, Manipulation und Verlust von Daten. Beim Drucken im Netzwerk lassen sich analog dazu Sicherheitsrisiken für Druckdaten während des Druckprozesses unter folgenden Gesichtspunkten betrachten:

▶ 1.1. Kompromittierung der Druckdaten

Druckdaten sind kompromittiert, wenn jemand Einsicht in diese Daten bekommt, für den sie nicht bestimmt sind. Zum Beispiel, wenn jemand unberechtigterweise Druckdaten als Klartext während der Datenübertragung im Netz mitliest.

▶ 1.2. Manipulation der Druckdaten

Druckdaten sind manipuliert, wenn während des Druckprozesses Inhalt und bzw. oder Form verändert werden. Es ist ohne großen Aufwand möglich, Druckjobs mit entsprechenden Hacker-Tools abzufangen und mit verändertem Inhalt weiter zu senden. Handelt es sich bei diesen Daten um Zahlungsanweisungen, Aufträge oder Ähnliches, kann offensichtlich großer Schaden angerichtet werden.

▶ 1.3. Verlust der Druckdaten

Unangenehme Folgen kann auch der Datenverlust haben, wenn zum Beispiel ein Druckjob verhindert und damit nicht ausgedruckt oder ein ausgedrucktes Dokument am Drucker entwendet wird. Geschäftsbedingte Druckvorgänge sind in der Regel notwendig und damit auch wichtig, zum Beispiel in der Logistik, Lagerhaltung und Kommissionierung. Angriffe auf dieser Ebene bringen finanzielle Nachteile für ein Unternehmen mit sich.³

Schäden, die durch solche Sicherheitsrisiken entstehen, sind in den meisten Fällen schwerwiegend: Materielle Schäden kosten Geld und Arbeitszeit (z. B. verzögerte Geschäftsprozesse, Wettbewerbsnachteile, rechtliche Konsequenzen), immaterielle Schäden schlagen sich in Form eines Imageverlustes nieder – oft genug ist beides nicht voneinander zu trennen. Dann spätestens stellt sich heraus: Die Kosten zur Einrichtung präventiver Sicherheitsmaßnahmen sind im Verhältnis zu den von solchen Schäden verursachten Kosten auf jeden Fall geringer. Es empfiehlt sich also, nach einer Risikoabschätzung auch zügig zu handeln und vorhandene Sicherheitslücken zu schließen oder zu minimieren. Dazu kommt, dass ein einmal etabliertes Sicherheitskonzept nur für eine begrenzte Dauer optimalen Schutz bietet. Da Angriffsmethoden sich ständig weiter entwickeln und neue hinzukommen, gilt es, sich ständig auf dem Laufenden zu halten: Was sind die aktuellsten Standards, welche neuen Sicherheitslösungen gibt es mittlerweile?

VDI Leitfaden

¹„Risikokommunikation für Unternehmen“, Hg. Dr. Peter M. Wiede-mann, Vorsitzender des VDI-Ausschusses „Technik - Risiko - Kommunikation“, Düsseldorf: VDI Verein Deutscher Ingenieure, 2000.

²Risikoabschätzung: „Eine Risikoabschätzung ist die Identifizierung, Quantifizierung und Bewertung von Risiken. Sie hat eine bestmögliche Prognose nach dem Stand des gegenwärtigen Wissens von Schäden im Hinblick auf die Wahrscheinlichkeit und das Ausmaß ihres Eintreffens zum Ziel.“ (a.a.O.)

IDC-Studie

³Laut der IDC-Studie „IT-Sicherheit im Mittelstand – Status Quo und Trends in Deutschland 2006“ ist die Vermeidung von Datenverlusten für den deutschen Mittelstand der Hauptantriebsfaktor für IT-Sicherheit.

2. DER DRUCKJOB IM NETZ: IM DSCHUNGEL DER SICHERHEITSRISIKEN

Um Sicherheitsrisiken beim Drucken im Netz zu identifizieren, ist ein Blick auf den Druckprozess bis hin zum Ausdruck aufschlussreich. Beim Drucken im Netz durchläuft ein Druckjob in einem Netz normalerweise folgende Stationen:

- ▶ Daten, Applikationen und Workstations
- ▶ Netzwerkzugang
- ▶ Netzwerkmedium (z. B. Kupferkabel, Glasfaser, WLAN)
- ▶ Netzwerkprotokolle (z. B. TCP/IP, HTTP)
- ▶ Netz-Subsysteme (z. B. Access Points, Hubs, Switches, Router, Gateways, Bridges, Netzwerkserver)
- ▶ Netzwerkdruckserver, Spooling Appliances, Printserver
- ▶ Drucker

An allen diesen Stationen gibt es Sicherheitsrisiken und Ansatzpunkte für Angriffe – aber eben auch Lösungen und geeignete Schutzmaßnahmen. Eine gründliche Risikoabschätzung klärt im Einzelfall, wo und in welchem Umfang Sicherheitsmaßnahmen notwendig und sinnvoll sind.

2.1. SICHERUNG VON DATEN, WORKSTATIONS UND APPLIKATIONEN

Die ersten Sicherheitsrisiken entstehen bei der Erstellung eines Druckdokuments. Hier geht es um Fragen wie: Auf welchem PC oder Notebook erstellt ein Anwender ein zu druckendes Dokument und wer hat zusätzlich noch Zugriff auf diesen Client? Gibt es einen Zugriffsschutz durch Login? Oder steht die Workstation in einem Raum, der abgeschlossen werden kann und zu dem nur bestimmte Personen Zugang haben?

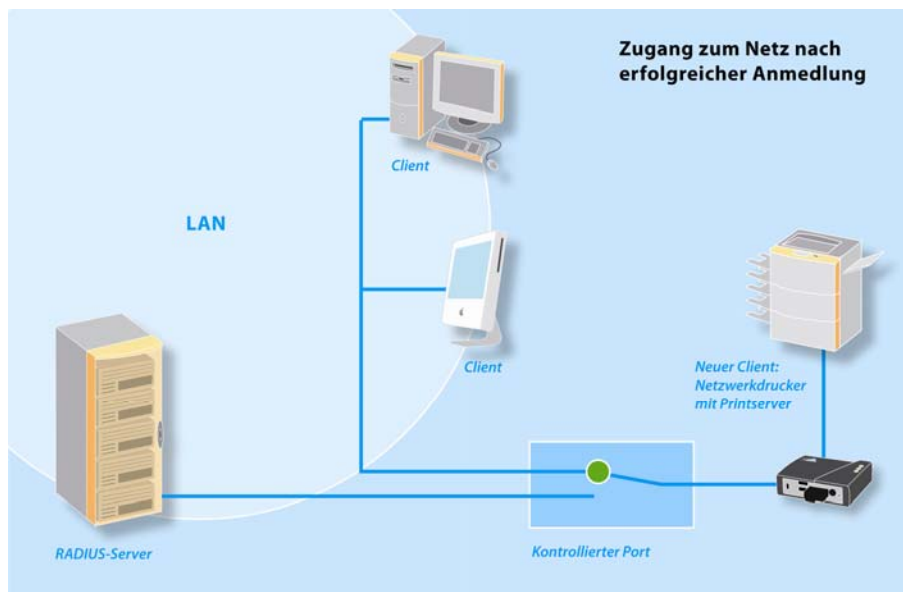
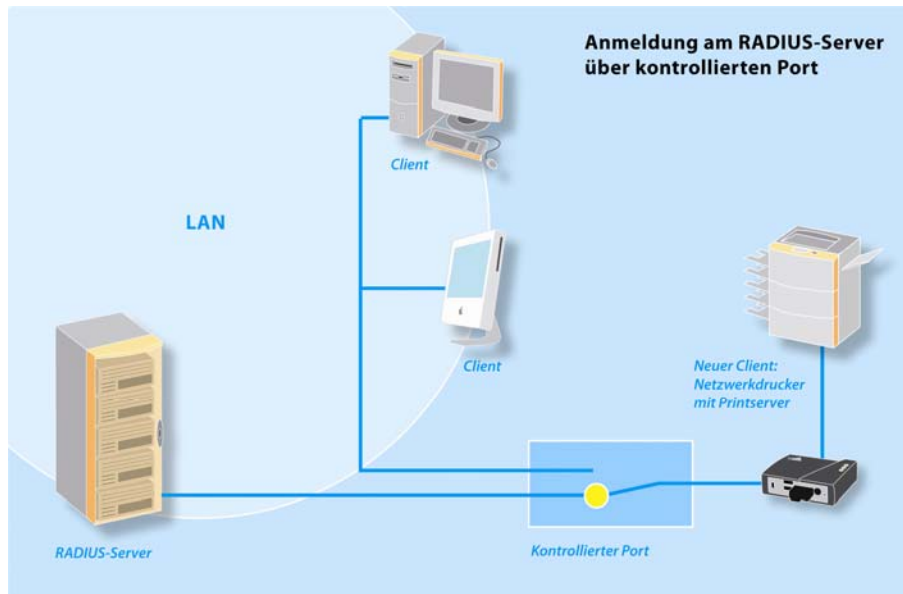
Die gleichen Fragen stellen sich in Hinblick auf die Zugangsberechtigungen zu Daten, Dokumenten und Applikationen. Manche Anwendungen, in denen ein zu druckendes Dokument erstellt wird, bieten mitunter auch schützende Funktionen wie Schreibschutz oder das Verbot zum Ausdrucken.

2.2. ZUGANG ZUM NETZ – MIT ODER OHNE KONTROLLE

Wenn der Zugang zum Netz für die Teilnehmer nicht geregelt ist, kann sich praktisch jeder ins Netz einklinken. Bei der Kontrolle des Zugangs sollten sowohl der physikalische als auch der logische Zugang zum Netz einbezogen werden.

- ▶ **Physikalischer Zugang zum Netz: Sicherung der Hardware:**
 - Verschießbare Verteilerschränke, abschließbare Patchdosen usw.
- ▶ **Logischer Zugang zum Netz:**
 - Autorisierung durch Administratoren mittels gerätebasierter Zugriffsregelungen über IP- oder MAC-Adressen via managed Switches bzw. Access Points – es bleibt das Restrisiko des unbefugten Zugriffs auf das Netz (z. B. Spoofing).

- Authentifizierung der Netzwerkteilnehmer durch benutzerbasierte Zugriffsregelungen mit zentraler Authentisierungsinstanz (Stichworte sind in diesem Zusammenhang IEEE 802.1x oder RADIUS-Server).



2.3. VOM NETZWERKTYP BEDINGTE SICHERHEITSRISIKEN

Die unterschiedlichen physikalischen Eigenschaften der gängigen Netzwerkmedien – Kupfer, Glasfaser und WLAN - bedingen spezifische Sicherheitsrisiken:

▶ **Kupfer:**

Die Datenübertragung erfolgt elektromagnetisch über Kupferkabel. Wenn ein Angreifer Zugriff auf das Kabel hat, kann er dieses direkt anzapfen. Elektronische Geräte und Netzkabel strahlen elektromagnetische Wellen ab, die so genannte Störstrahlung. Darin sind im Falle von Geräten, die Informationen verarbeiten - PCs, Faxgeräten, Modems etc. - auch die übertragenen Informationen enthalten. Dieses Phänomen der „bloßstellenden Abstrahlung“ nutzen Hacker für das Mitlesen von Daten im Netz. Spezielle Abschirmungen und Entstörungsaufwendungen können das verhindern.

▶ **Glasfaser:**

In Glasfasernetzen erfolgt die Datenübertragung optisch (daher engl. Fiber Optics) mittels der so genannten Totalreflexion, bei der Licht nahezu verlustfrei reflektiert, also „geleitet“, wird (Lichtwellenleiter, LWL-Technologie). Da bei dieser Technologie keine elektromagnetische Abstrahlung entsteht, gilt sie als abhörsicher. Ein „Anzapfen“ des Kabels, beispielsweise über das Aufschneiden (Splicing) oder Biegen (Coupler- oder Splitter-Methode) der Leitung, lässt sich aufgrund der daraus resultierenden Dämpfung umgehend feststellen. Abhörmethoden ohne Zugriff auf das Kabel (z.B. Non-Touching Methode) sind unverhältnismäßig aufwändig. Wer sich allerdings auch gegen solche „Optical Tapping“-Angriffe schützen möchte, muss die übertragenen Daten zusätzlich verschlüsseln.

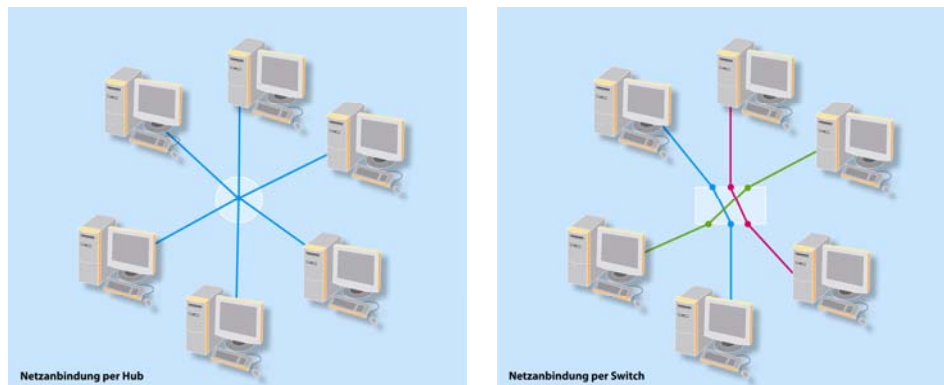
▶ **WLAN:**

WLAN (Wireless Local Area Network) basiert auf der Funktechnologie, in der Regel nach einem Standard der IEEE 802.11-Familie. In diesem Fall gibt es kein Kabel, das manipuliert werden kann. Stattdessen besteht die Datenübertragung an sich komplett aus Funkwellen. Um Daten im WLAN zu schützen, sind zum einen die Authentifizierung des Netzteilnehmers am Access Point (s. o.) und zum anderen die Verschlüsselung der Daten wichtig. Die zurzeit gebräuchlichsten WLAN-Verschlüsselungstechniken sind WEP und WPA bzw. WPA2.

- **WEP (Wired Equivalent Privacy, IEEE-Standard 802.11):** Diese Verschlüsselungsmethode basiert auf dem RC 4 Algorithmus und gilt mittlerweile nicht mehr als sicher, ist jedoch noch weit verbreitet.
- **WPA und WPA2 (Wi-Fi Protected Access):** WPA nimmt in Teilen den neuen Sicherheitsstandard 802.11i vorweg, um die bekannten Sicherheitslücken von WEP zu schließen. Der vollständige IEEE-Standard 802.11i ist mit WPA2 umgesetzt, das zudem mit dem noch sichereren Verschlüsselungsalgorithmus AES (Advanced Encryption Standard, Rijndael-Algorithmus) arbeitet. Die bedeutendste Sicherheitsfunktion von WPA ist der Schutz durch dynamische Schlüssel. Diese basieren auf dem Temporal Key Integrity Protocol (TKIP). WPA bzw. WPA2 sind zurzeit die modernsten, sichersten und am weitesten verbreiteten Verschlüsselungsstandards für WLAN.

2.4. NETZ-SUBSYSTEM – SICHERHEIT DURCH NETZWERK-KOMPONENTEN

Der verwendete Netzwerktyp definiert zum Teil auch notwendige Komponenten des Netz-Subsystems wie Hubs, Switches, Server, Verkabelung, Access Points etc. Beispielsweise ist ein Switch auf jeden Fall sicherer als ein Hub, weil er wie eine Telefonvermittlung arbeitet (mindestens OSI-Schicht 2) und nicht wie ein Hub jedes Datenpaket an alle angeschlossenen Ports weitergibt (OSI-Schicht 1).



Bei einem WLAN-Access Point ist die Ausstattung ausschlaggebend für die Sicherheit: Bietet der Access Point nur schwache oder auch starke Verschlüsselungsstandards, Authentifizierungsverfahren etc.

Für die Komponenten des Netz-Subsystems gilt ebenfalls, dass sowohl der physikalische Zugriff als auch die Zugriffsregelungen via IT-Administratoren Eingang in die Risikoabschätzung finden sollten.

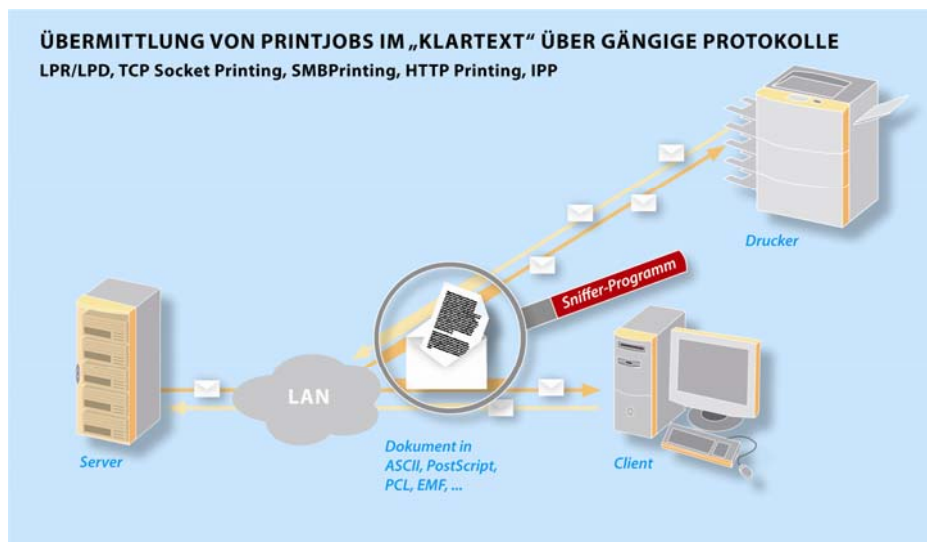
2.5. NETZWERKPROTOKOLLE MIT INTEGRIERTEN SICHERHEITSMCHANISMEN

Die Netzwerkkommunikation lässt sich mit dem OSI-Schichtenmodell beschreiben (Open Systems Interconnection Reference Model; auch OSI/ISO-Modell, OSI-Referenzmodell, 7-Schichten-Modell). Darin werden die unterschiedlichen Bereiche der Netzwerkkommunikation zur geregelten Reihenfolge bei der elektronischen Signalübertragung in sieben aufeinander aufsetzende Schichten unterteilt. Die Kommunikation erfolgt über Netzwerkprotokolle, die sich in den OSI-Schichten 3 bis 7 bewegen. Viele der Protokolle, die beim Drucken im Netz Verwendung finden, enthielten in ihrer Ursprungsform keine Verschlüsselungs- oder Sicherheitsmechanismen. In neueren Versionen sind bei einigen Protokollen Sicherheitsmechanismen integriert. Beispiele dafür sind unter anderem:

- ▶ http → HTTPs
- ▶ FTP → secure FTP
- ▶ IPP → IPP v1.1
- ▶ SNMP → SNMP v3
- ▶ IP → IPv6, IPsec

2.6. DRUCKDATENVERSCHLÜSSELUNG MIT SSL/TLS

Bei den im vorigen Abschnitt erwähnten Sicherheitsmechanismen handelt es sich in der Regel um Autorisierungs- und Authentifizierungsverfahren oder um die Verschlüsselung von Rohdaten. Um zu vermeiden, dass Druckdaten im Klartext durch das Netz geschickt werden, müssen sie verschlüsselt werden, denn letztendlich überträgt jedes Druckprotokoll mehr oder minder Klartext (z. B. ASCII, PCL, Postscript).



Herstellerübergreifend gibt es zur Verschlüsselung der Druckdaten nur das Internet Printing Protokoll (IPP) in der aktuellen Version 1.1, welches in den RFCs 2910, 2911 und 3196 beschrieben ist. IPP v1.1 basiert auf HTTP 1.1 und kann alle Erweiterungen für HTTP verwenden. Dazu gehört der Einsatz von SSL/TLS zur Verschlüsselung. Allerdings unterstützen die aktuellen Windows-Betriebssysteme das Protokoll IPP v1.1 nicht. Windows 2000, XP Professional und Windows Server 2003 können den Webserver IIS als Windows-Komponente in der Software-Rubrik der Systemsteuerung nachinstallieren. Dieser lässt sich auch als Druckserver konfigurieren und ermöglicht das Drucken über IPP sowie die SSL-verschlüsselte Druckdatenübermittlung über das Internet. Angeschlossene Netzwerkdrucker werden über ein Webinterface verwaltet.

In Linux- und Unix-Umgebungen wird IPP v1.1 von CUPS (Common Unix Printing System) unterstützt. Ein weiteres Beispiel für die Unterstützung von IPP v1.1 ist die Betriebssystemerweiterung RSO Spool für das Mainframesystem BS2000 OSD von Fujitsu Siemens.

Darüber hinaus gibt es lediglich einzelne proprietäre Lösungen zur verschlüsselten Druckdatenübertragung.

2.7. ZUGRIFFSRECHTE AUF DAS OUTPUT-GERÄT

Der Zugriff auf den Drucker sollte in ein durchgängiges Konzept zum sicheren Netzwerkdruck mit einbezogen sein. Der physikalische Zugriff auf Drucker kann beispielsweise durch das Aufstellen in verschließbaren Räumen kontrolliert werden. Den logischen Zugriff auf ein Output-Gerät regeln bereits angesprochene Verfahren zur Authentisierung oder Authentifizierung, die analog auch für den Drucker gelten. Beispielsweise können Administratoren über eine Funktion zur Filterung von Client-IP-Adressen gewährleisten, dass nur diejenigen Mitarbeiter auf einen Farbdrucker zugreifen können, für die es beruflich notwendig ist. So lässt sich auch verhindern, dass gehackte Druckjobs von unberechtigter Seite auf einem Drucker ausgegeben werden.

2.8. AUSGABE DES DRUCKDOKUMENTS AM DRUCKER AN BERECHTIGTE ANWENDER

Ist der Druckauftrag einmal unterwegs, hilft auch die Verschlüsselung der Druckdaten nicht vor unberechtigtem Zugriff, wenn der Ausdruck am Drucker selbst ungeschützt im Fach landet – und für jedermann einsichtig ist oder einfach entfernt werden kann. Die Lösungen reichen von Face Down Printing, bei dem das Dokument mit dem Text nach unten ausgegeben wird, bis zu den weit verbreiteten Follow-Me-Printing- oder Private Printing-Lösungen, bei denen sich berechnigte Adressaten eines Druckdokumentes am Drucker identifizieren müssen. Das geschieht mit verschiedenen Mitteln, die sich mitunter kombinieren lassen:

- ▶ PIN
- ▶ Magnet oder Chipkarten
- ▶ Berührungslose Karten (z. B. RFID)
- ▶ Biometrische Verfahren (z. B. Fingerabdruck)

Einen Sonderfall stellt TEMPEST (Temporary Emanation and Spurious Transmission oder Transient Electromagnetic Pulse Emanation Standard) dar: Dabei handelt es sich um eine vollständige Abschirmung des Druckers von elektromagnetischer Strahlung mittels einer isolierenden Umhüllung. Zugleich wird damit in der Regel ein unberechtigter Zugriff auf ein Druckdokument unmöglich gemacht.

3. SICHERE NETZWERK-DRUCKLÖSUNGEN VON SEH IM ÜBERBLICK

Die Lösungen von SEH zum sicheren Drucken im Netzwerk setzen an vier Punkten an:

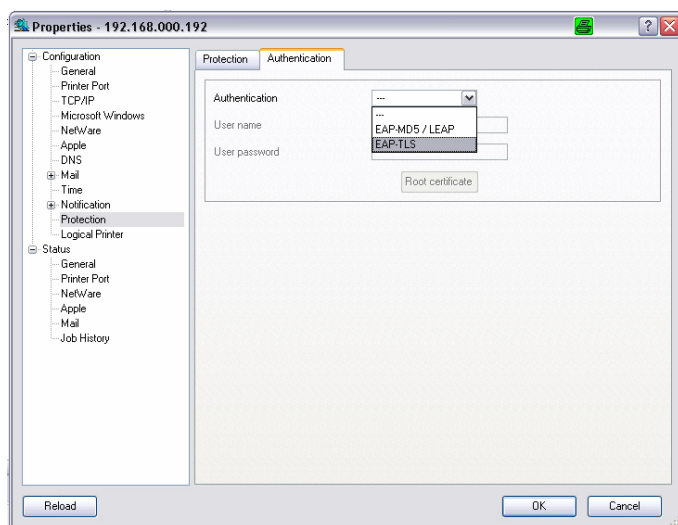
- ▶ spezielle Lösungen für bestimmte Netzwerkmedien (Glasfaser, WLAN)
- ▶ Systemschutz (Authentifizierung, Konfigurationsschutz, Zugriffsrechte)
- ▶ Schutz der Druckdaten durch Druckdatenverschlüsselung
- ▶ Private Printing-Lösung zur sicheren Dokumentenausgabe

3.1 SEH PRINTSERVER FÜR BESTIMMTE NETZWERKMEDIEN

- ▶ **Glasfaser:** Das Drucken im Netz profitiert mit abhörsicheren Glasfaserverbindungen bis an den Drucker (Fiber-to-the-Desk, FTTD) von allen Vorteilen, welche Glasfaser bietet – besonders von der Sicherheit bei der Datenübertragung. SEH bietet das weltweit umfassendste Portfolio sowohl an internen als auch an externen Printservern. Mit solchen Lösungen können Anwender ein auf Glasfaser basierendes Sicherheitskonzept bis zum Drucker umsetzen.
- ▶ **WLAN:** Die WLAN-Verschlüsselungsstandards der IEEE 802.11-Familie sind ebenfalls in allen Modellen der SEH WLAN-Produktpalette implementiert. Während die älteren Produkte mit WEP ausgestattet sind, verfügen die WLAN-Printserver der jüngsten SEH Printserverlinie über die neueren und sichereren Verschlüsselungsstandards WPA und WPA2, sind jedoch auch rückwärtskompatibel zu WEP.

3.2 BENUTZER-AUTHENTIFIZIERUNG

Als Schnittstelle vom Drucker zum Netzwerk sorgen SEH Printserver sowie das ThinPrint Gateway TPG60 dafür, dass sich die Geräte korrekt am Netzwerk anmelden. Bei der Kommunikation eines Clients mit einem dieser Geräte lässt sich die Identität des letzteren sicher bestimmen. Dabei handelt es sich um eine Zwei-Port-Authentifizierung auf der Basis der Implementierung von IEEE 802.1x. Dieses Verfahren ist typisch für die WLAN-Technologie, in der die Authentifizierung über Access Point und RADIUS Server erfolgt. Es findet zunehmend auch in Kabelnetzen Verwendung, wobei ein Switch die Aufgabe des Access Points übernimmt.

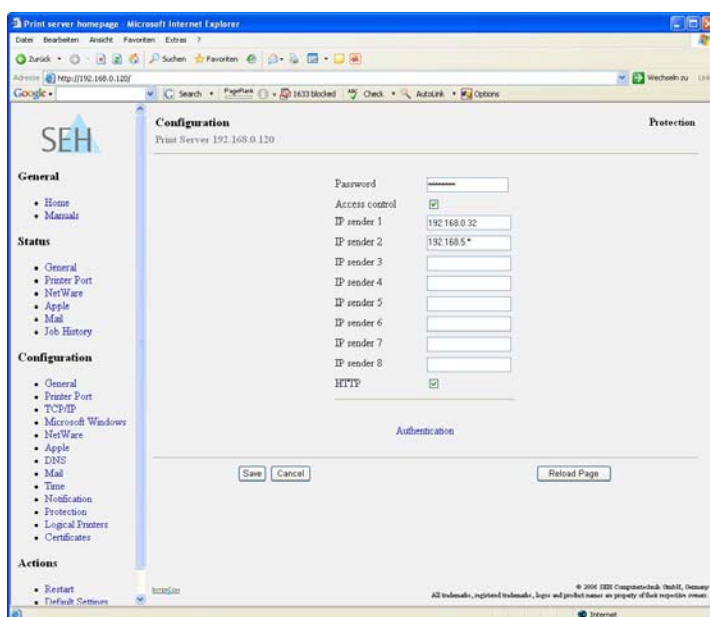


3.3 ZUGRIFFS- UND KONFIGURATIONSSCHUTZ DER SEH PRINTSERVER

Weil Printserver für die Sicherheit beim Netzwerkdruck eine wichtige Rolle spielen können, hat SEH Funktionen zur Regelung der Zugriffsrechte auf die Konfiguration der Printserver implementiert. Ein Passwortschutz sichert die Konfiguration eines Printservers wirkungsvoll und einfach vor Manipulation und nicht berechtigtem Zugriff ab. So können zwar alle Netzwerkteilnehmer über die Management-Optionen Einsicht in die Konfiguration eines Printservers nehmen (z. B. über Browser, das SEH InterCon-NetTool oder herstellereigene Management-Tools) - Änderungen der Konfiguration können jedoch nur mit der vorherigen Eingabe eines festgelegten Passworts vorgenommen werden. Printserver von SEH bieten mit der Funktion „Zugangskontrolle“ (Access Control) zusätzlich die Möglichkeit, die Konfiguration eines Printservers per Mausklick für nicht zugriffsberechtigte Netzwerkteilnehmer unsichtbar zu machen. Bei einigen Druckermodellen lässt sich mit dieser Funktionalität auch die Konfiguration des Printservers via Druckerpanel sperren.

3.4 ZUGRIFFSSCHUTZ AUF DRUCKER

SEH Printserver verfügen über die Filterfunktion IP Sender. Sie schützt Drucker vor unberechtigter Nutzung, indem nur bestimmte IP-Adressen – und damit User-Arbeitsplätze - Zugriffsrechte auf einen Netzwerkdrucker bekommen. Dazu stehen Felder zur Eingabe von IP-Adressen oder Hostnamen beziehungsweise zur Eingabe von IP-Adressbereichen via „Wild Card“ zur Verfügung.



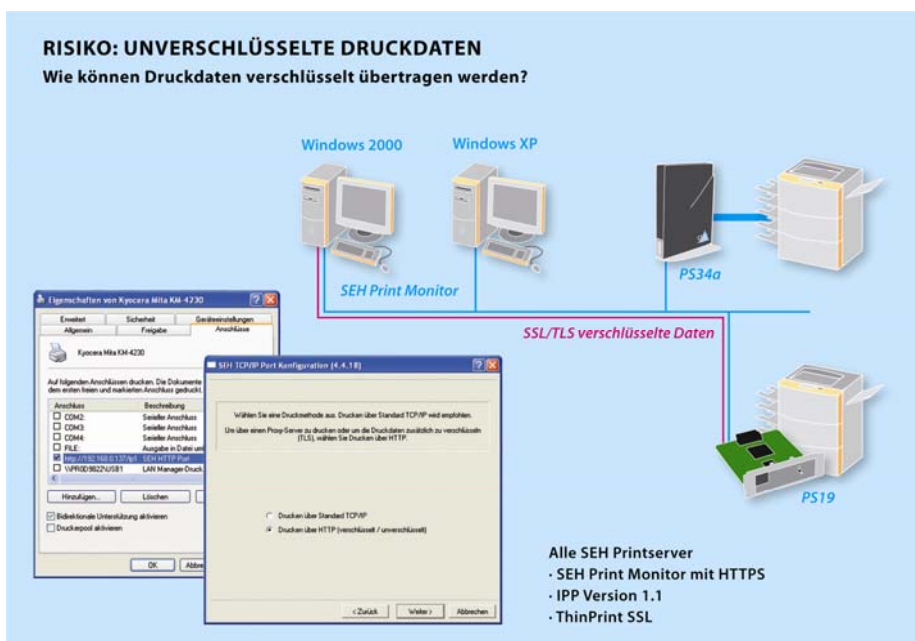
Auf diese Weise können Administratoren die Anwendergruppe präzise definieren: Von einzelnen Usern über kleine Gruppen bis hin zu ganzen Abteilungen lässt sich so der Zugriff auf bestimmte Drucker festlegen.

3.5 DRUCKDATENVERSCHLÜSSELUNG MIT SSL/TLS (128 BIT-VERSCHLÜSSELUNG)

Der SEH Print Monitor ist eine selbst entwickelte Software für Windows-Betriebssysteme, welche Druckjobs verschlüsselt. Windows Clients haben mit diesem Tool die Wahl zwischen Socket Printing (Port 9100) oder HTTP Printing (Port 80). Bei HTTP Printing können Nutzer entscheiden, ob sie unverschlüsselt (Port 80) oder verschlüsselt über HTTPS (Port 443) drucken möchten.

Für den Einsatz mit anderen Betriebssystemen wie Mac OS oder Linux bieten SEH Printserver Druckdatenverschlüsselung mit dem etablierten Standard IPP v1.1.

Ein weiteres Beispiel für proprietäre Verfahren ist die kürzlich von ThinPrint entwickelte ThinPrint SSL-Verschlüsselung, welche das Unternehmen in seine Lösung zum bandbreitenoptimierten Drucken integriert hat. Bisher ist SEH der einzige Anbieter, dessen jüngste Printserverfamilie ThinPrint SSL unterstützt.



3.6 FOLLOW ME PRINTING-LÖSUNG MIT SEH PRINTSERVER

Einige SEH Printserver für Kyocera-Drucker lassen sich mit dem Identifikations- und Abrechnungssystem „Card’n’Print / Card’n’Copy“ von M.S.E. kombinieren. Das M.S.E. „Card’n’Print“ wird mittels eines speziellen Anschlusses mit dem SEH-Printserver verbunden. Bei dieser Lösung werden die Druckjobs der jeweiligen Anwender auf eine spezielle M.S.E. Server-Komponente gespoolt. Die Anwender authentifizieren sich mit einer M.S.E.-Magnetkarte am Drucker. Wenn der Nutzer berechtigt ist, werden die Druckjobs freigestellt. Auf diese Weise ist sicher gestellt, dass nur berechtigte Anwender auf bestimmte Drucker zugreifen können. Gleichzeitig kann dieses System auch zum Druckkosten-Controlling verwendet werden.

4. LÖSUNGEN FÜR SICHEREN NETZWERKDRUCK VON SEH AUF EINEN BLICK:

SPEZIELLE LÖSUNGEN FÜR BESTIMMTE NETZWERKMEDIEN:

- ▶ Glasfaser: Printserver für abhörsichere Fiber-to-the-Desk Netzwerkdruck-Lösungen
- ▶ WLAN-Printserver mit Authentisierungsprotokoll-Unterstützung (EAP-MD5, EAP-TLS, Cisco LEAP) und Verschlüsselungsstandards (WEP, WPA, WPA2)

SYSTEMSCHUTZ:

- ▶ Benutzerauthentifizierung (IEEE 802.1x)
- ▶ Zugriffs- und Konfigurationsschutz für SEH Printserver
- ▶ Zugriffsschutz für Drucker (IP-Sender)

SCHUTZ DER DRUCKDATEN DURCH DRUCKDATENVERSCHLÜSSELUNG MIT SSL/TLS (128 BIT-VERSCHLÜSSELUNG)

- ▶ SEH Print Monitor für aktuelle Windows-Betriebssysteme
- ▶ IPP v1.1-Implementierung für Mac OS, Linux und andere Betriebssysteme
- ▶ ThinPrint SSL-Verschlüsselung

DOKUMENTENZUGRIFF

- ▶ Kombination SEH Printserver und M.S.E. „Card’n’Print Card’n’Copy“ für Kyocera Drucker und MFG zur Ausgabe von Dokumenten an berechtigte Nutzer

5. LITERATUR

- ▶ Eberlein, Dieter, u. a.: Lichtwellenleiter-Technik, Dresden: expert verlag, 2003
- ▶ IDC-Studie "IT-Sicherheit im Mittelstand – Status Quo und Trends in Deutschland 2006"
- ▶ Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector, US Secret Service and CERT Coordination Center, 2005
- ▶ Nestler, Claudia und Steffen Salvenmoser: Wirtschaftskriminalität 2005, Hg. PricewaterhouseCoopers AG WPG, Frankfurt am Main, in Zusammenarbeit mit der Martin-Luther-Universität Halle-Wittenberg, 2005
- ▶ RFC 2828: Internet Security Glossary
- ▶ Richter, Lars: Untersuchung und Bewertung von Netzzugangssteuerungen auf Basis des Standards 802.1x (Port-Based Network Access Control), Chemnitz: Technische Universität Chemnitz, Diplomarbeit, 2005
- ▶ VDI Leitfaden „Risikokommunikation für Unternehmen“, Hg. Dr. Peter M. Wiedemann, Vorsitzender des VDI-Ausschusses „Technik – Risiko -Kommunikation“, Düsseldorf: VDI Verein Deutscher Ingenieure, 2000

6. INTERNET

- ▶ Zu Glasfaser: www.glasfaser.de
- ▶ Zum Internet Printing Protocol (IPP v1.1): www.pwg.org/ipp
- ▶ Zu Wi-Fi Protected Access (WPA/WPA2): www.wi-fi.org