

IT-Security in Deutschland 2010

Deutschland 2010

.....
Unternehmensdarstellung und Fallstudie: Hewlett Packard
.....

- ANGABEN OHNE GEWÄHR -

IDC Multi-Client-Projekt ▪ Juli 2010 ▪ Analyst: Lynn-Kristin Thorenz

METHODIK

Das nachfolgend dargestellte Unternehmensprofil sowie die Fallstudie basieren auf Informationen, die von HP zur Verfügung gestellt wurden. Für diese Angaben übernimmt IDC keine Gewähr.

HEWLETT-PACKARD (HP)

Unternehmensdarstellung HP

Informationen zum Unternehmen

HP ist eines der weltweit größten Technologie-Unternehmen. Das Produktangebot umfasst die Bereiche Drucken, Personal Computing, Software, Services und IT-Infrastruktur und richtet sich an Privatpersonen und Unternehmen.

Um die Entwicklung und den Ausbau von HP MPS (**M**anaged **P**rint **S**ervices) voran zu treiben, gründete HP eine eigene Managed Enterprise Solutions (MES) Sparte. Hierdurch soll die Endkundenbetreuung gestärkt werden. Zudem strebt HP an, das Mittelstandsgeschäft durch eine dedizierte Vertriebsmannschaft und entsprechende Partnerprogramme auszubauen.

Positionierung im Bereich IT Security

HP ist ein Lieferant von Bildbearbeitungs- und Drucklösungen für große Organisationen. Das Unternehmen bietet technisches Fachwissen sowie Produkte und Lösungen an – auch rund um das Thema Drucker- und Dokumentensicherheit. Drucker sind heutzutage wie PCs oder Laptops in das Unternehmensnetzwerk eingebunden und können damit ebenso wie Rechner gehackt werden. HP unterstützt Unternehmen nach eigenen Angaben dabei, ihre Output Management-Architektur sicher zu gestalten und den Mitarbeitern trotzdem eine effiziente Infrastruktur anzubieten. Neben der Hardware bietet HP

- Beratungsservices, einschließlich Beschaffung, Installation, Verwaltung und Support, die an die Anforderungen der Kunden angepasst werden und dazu beitragen können, die Effektivität eines Unternehmens zu steigern.
- Leistungsfähige Lösungen, die die Firmenumgebung optimieren, Geschäftsergebnisse steigern und die Umwelt schützen können.

Dies gilt auch für den Bereich Druckersicherheit. HP entwickelt und implementiert auf die Firmenanforderungen zugeschnittene Lösungen. Ausgangspunkt ist nach Angabe von HP eine detaillierte Analyse der Ausgangslage, auf Basis derer zusammen mit dem Kunden eine entsprechende Sicherheitsarchitektur entwickelt und implementiert wird.

Darstellung des IT Security Portfolios

Da die meisten Drucker heute im Netzwerk integriert sind, sind sie genauso anfällig wie PCs wenn es um das Thema Sicherheit geht. Sie lassen sich von außen hacken, die größte Gefahr geht jedoch von den eigenen Mitarbeitern aus – absichtlich oder unabsichtlich. Denn gerade die Druckersicherheit wird in Unternehmen oftmals stiefmütterlich behandelt. Viele Mitarbeiter denken beispielsweise nicht darüber nach, ob ein im Schacht vergessener Ausdruck nicht vielleicht in falsche Hände gerät – oder zumindest von einem Mitarbeiter gelesen wird, der diese Dokumente normalerweise nicht sehen sollte und würde. Um dies zu verhindern, kann zum Beispiel eine Lösung zum sicheren Drucken eingeführt werden: Bevor der Ausdruck gestartet wird, muss der Mitarbeiter sich zunächst am Gerät anmelden, wozu er z.B. seinen Mitarbeiterausweis oder eine Pin verwendet. Ein weiterer Vorteil dieses Drucks auf Abruf: doppelte Ausdrücke gehören der Vergangenheit an und der Papierverbrauch sinkt zusätzlich. Darüber hinaus lässt sich das gewünschte Dokument an jedem Netzwerkdrucker im Unternehmen ausdrucken.

Bevor es jedoch an die Implementierung von Sicherheitslösungen geht, sollten Anwenderrichtlinien entwickelt werden. Diese regulieren bereits die Nutzung von E-Mail, Internet, Telefon, Instant Messaging und anderen Geräten – darunter auch Drucker. Leitfäden mit „Good Practice“ Beispielen im Hinblick auf Datenerstellung, Speicherung, Transport und Nutzung sind unternehmenskritisch, da es immer häufiger interne Sicherheitslecks gibt. Das Resultat: Es ist extrem wichtig, dass Mitarbeiter AUP-Trainings erhalten, um diese Richtlinien effektiv umzusetzen. Die meisten Angestellten realisieren nicht, dass für Drucker die gleichen Sicherheitsrisiken gelten wie für PCs – hier muss ein Umdenken stattfinden.

Sichere Druckrichtlinien sollten alle Aspekte des Prozesses berücksichtigen, vom Erstellen der Inhalte und ihrem Druck bis hin zum physischen Schutz der Geräte und des Zubehörs. In vielen Unternehmen sind dafür zwei verschiedene Abteilungen verantwortlich: Die IT für Geräte und Netzwerk, während sich das Gebäudemanagement um den Schutz vor Diebstahl und physische Schäden kümmert. Beide Abteilungen sollten aber eng zusammenarbeiten, da ihre Rollen sich im Hinblick auf die Druckumgebung ergänzen. Dies ist auch bei Sicherheitsüberprüfungen für das jeweilige Unternehmen ein deutlicher Vorteil. Allerdings haben keine zwei Unternehmen deckungsgleiche Anforderungen an sichere Druckumgebungen. Je nach Größe oder Branche haben Firmen verschiedene Sicherheitsansprüche. HP stellt bei seiner Analyse der Ausgangssituation beispielsweise folgende Fragen, um die Anforderungen des Kunden einzuschätzen:

- Welche Art von Dokumenten wird am häufigsten gedruckt – interne oder solche für Kunden?
- Sind die Dokumente zur Information (Broschüren) oder eher rechtsverbindlich (Verträge)?
- Gibt es in der jeweiligen Branche ein erhöhtes Risiko im Hinblick auf Sicherheitsverstöße?
- Welcher Prozentanteil der gedruckten Dokumente ist vertraulich?
- Wie sieht die Unternehmensdynamik aus? Ist sie Büro-basiert, Kunden-gerichtet oder auf Remote-Arbeiten ausgerichtet? Welche Auswirkungen hat diese Dynamik für die Druckumgebung?

Auf Basis dieser Analyse erstellt der Druckspezialist anschließend eine maßgeschneiderte Architektur, die beim Kunden realisiert wird. Dazu gehören neben Authentifizierung, Drucken auf Abruf auch das Thema zentrale Administration und Überwachung der Geräte.

Referenzen im Bereich IT Security (in Deutschland)

- Kunde1: Nestlé Purina PetCare
- Kunde 2: Stadt Stralsund

Fallstudie: Hansestadt Stralsund

Informationen zum Kunden

Die Verwaltung der Hansestadt Stralsund ist über zehn Standorte verteilt. Rund 600 Mitarbeiter teilen sich 350 Output-Systeme, vom Arbeitsplatz- über Abteilungsdrucker bis zu Kopierern und Faxgeräten.

Anforderungen des Kunden

Die Stadt Stralsund wünschte sich eine Konsolidierung ihrer bisherigen Druckerlandschaft, die einerseits Aufgaben von Kopierern und Faxgeräten übernehmen kann, andererseits so moderne Features wie den Follow-Me-Druck (Start und Erledigung des Druckjobs an zwei unterschiedlichen Standorten) und ein Authentifizierungssystem bietet. HP erfüllte diese Vorgaben und man setzte den Konsolidierungsprozess in die Realität um.

Darstellung der Lösung

Ziel war die Konsolidierung des Output Managements mit Einführung automatisierter Druck- und Authentifizierungsverfahren. HP realisierte die Anforderungen des Unternehmens durch den weitgehender Wegfall dedizierter Arbeitsplatzdrucker im Back-Office-Bereich. Gleichzeitig ersetzte der Managed Print Services Spezialist den Kopierer-,Scanner- und Faxgerätepark durch Multifunktionsgeräte. Besonderen Wert legte die Stadt Stralsund auf die Sicherheit von Daten und Ausdrucken. HP implementierte hier Systeme mit Follow-Me- und Authentifizierungsmöglichkeiten. Dokumente lassen sich jetzt nur dann ausdrucken, wenn sich der Mitarbeiter vorher am Drucker authentifiziert. So ist nicht nur die Sicherheit und Vertraulichkeit gedruckter Informationen gewahrt, sondern auch die Anzahl der im Gerät vergessenen Dokumente sinkt.

Projekthighlights

- Deutliche besserer Workflow durch Follow-Me-Druck über verschiedene Standorte hinweg.

- ☒ Größtmögliche Datensicherheit durch Authentifizierungssysteme an ausgewählten LaserJets.
- ☒ Gegenüber vorherigen Lösungen bessere Druckqualität bei größerer Performance.
- ☒ Jährliche Kosteneinsparung gegenüber der vorherigen Ausstattung von mehreren tausend Euro.
- ☒ Keine Kapitalbindung durch HP Smart Printing Services mit monatlichen Fixkosten.

Zitate des Kunden zum Projekt

- ☒ „Überzeugt haben uns vor allem die HP MFPs, von denen wir vier verschiedene Modelle im Einsatz haben. Sie sind mit einem Authentifizierungssystem auf Transponder-Basis ausgerüstet. Das heißt: Kommt ein registrierter Mitarbeiter mit seinem beispielsweise am Schlüsselbund hängenden Transponder in die Nähe eines HP MFP, weiß das System sofort, um wen es sich handelt. Der Druck-, Kopier- oder Faxjob kann ohne manuelles Zutun sofort dem jeweiligen Mitarbeiter zugeordnet werden.“
- ☒ „Wenn zum Beispiel ein Mitarbeiter am Standort A über seinen PC Ausdrucke startet, kann er bestimmen, dass das Dokument am Standort B aus dem Drucker kommt. Und zwar erst dann, wenn er sich als Urheber diesem System gegenüber legitimiert hat. Damit ist der Datenschutz größtmöglich gewährleistet. Nicht abgeholte Ausdrucke, auf die jeder Vorbeikommende einen Blick werfen kann, gibt es bei uns nicht mehr.“
- ☒ „HP hat genau das realisiert, was wir benötigen – und das zu unschlagbaren Konditionen. Schade, dass wir nicht schon eher darauf gekommen sind ...“

Gabriele Leesch, Abteilungsleiterin EDV in der Stadtverwaltung Stralsund.

Copyright Hinweis

Die externe Veröffentlichung von IDC Information und Daten – dies umfasst alle IDC Daten und Aussagen, die für Werbezwecke, Presseerklärungen oder anderweitige Publikation verwendet werden, setzt eine schriftliche Genehmigung des zuständigen IDC Vice Presidents oder des jeweiligen Country-Managers bzw. Geschäftsführers voraus. Ein Entwurf des zu veröffentlichenden Textes muss der Anfrage beigelegt werden. IDC behält sich das Recht vor, eine externe Veröffentlichung der Daten abzulehnen.

Für weitere Informationen bezüglich dieser Veröffentlichung kontaktieren Sie bitte: Katja Schmalen, Marketing Manager, +49 (0)69/905020 oder kschmalen@idc.com.

Urheberrecht: IDC, 2010. Die Vervielfältigung dieses Dokuments ist ohne schriftliche Erlaubnis strengstens untersagt.