

Datendiebstahl immer einen Schritt voraus

Landeskriminalamt Saarland hat mobile Endgeräte mittels Device Management sicher im Griff

Daten sind mobil und transportabel geworden, im wahrsten Sinne des Wortes. Auch große Datenbanken passen heute auf eine Speicherkarte von der Größe eines Daumennagels, der universelle Einsatz solcher Speicher macht selbst Mobiltelefone, Digitalkameras oder MP3-Player zum Werkzeug für Datendiebstahl im großen Stil. Insbesondere das Aufkommen der USB-Schnittstelle und die erhöhte Datentransferrate in USB 2.0 haben dazu beigetragen, dass Dateien und Anwendungen schnell und einfach auf die unterschiedlichsten Endgeräte übertragen werden können. Natürlich ist diese Entwicklung segensreich und enorm praktisch für viele Einsatzgebiete, aber sie birgt auch erhebliche Risiken in sich. Neben Datendiebstahl betrifft das auch die unkontrollierte Übertragung von Schadprogrammen wie Trojaner oder Viren. Dieser Beitrag schildert, wie das Landeskriminalamt (LKA) Saarland diese Risiken mit intelligentem Device-Management in den Griff bekommen hat.

Das LKA Saarland, das 2007 sein 50jähriges Jubiläum feierte, ist einerseits wichtiger Träger der operativen Kriminalitätsbekämpfung und andererseits zentrale Dienststelle im Sinne des BKA-Gesetzes für das Saarland. Zu den Arbeitsbereichen zählen Fahndungen, Ermittlungen, Beweissicherungen, aber auch Prävention und Opferschutz. Im Jahr 2007 wurden bei der Polizei des Saarlandes 73.813 registrierte Straftaten bearbeitet von denen über 52 Prozent aufgeklärt werden konnten.

Informationen als Basis moderner Verbrechensbekämpfung

Im Zentrum polizeilicher Arbeit stehen seit je her Informationen. Ohne verifizierte und aktuelle Informationen ist eine nachhaltige Verbrechensbekämpfung nicht möglich. Grundlage für den Erfolg der Polizei ist eine schnelle Reaktionsfähigkeit in Bezug auf gesellschaftliche Veränderungsprozesse, technologischen Wandel und die sich ständig verändernde Kriminalität. Um so effektiv wie möglich arbeiten zu können, muss das LKA als zentraler IT-Dienstleister für die beiden Polizeibehörden Landespolizeidirektion (LPD) und das LKA selbst Zugang zu sensiblen Daten gewähren. Dem allgemeinen Trend folgend haben daher auch mobile Endgeräte und Speichermedien Einzug in den Arbeitsalltag gehalten. Der Einsatz dieser Geräte ermöglicht einerseits die effiziente Verbrechensbekämpfung, stellt andererseits jedoch eine Schwachstelle dar. Das wirft natürlich Sicherheitsfragen auf. Seit März 2007 setzt man daher auf die Device Management Lösung devicepro® und stellt so sicher, dass nur berechnigte Personen mit zugelassenen mobilen Endgeräten Zugriff auf Daten erhalten.

Mobile Endgeräte verändern Bedrohungspotenzial

Nach außen hin ist die Polizei des Saarlandes durch die üblichen Sicherheitsmaßnahmen wie Firewall, Antiviren-Software und regelmäßige Aktualisierungen seiner Software geschützt. Auch die Netzwerke unterliegen höchsten Sicherheitsstandards, wie sie das BSI (Bundesamt für Sicherheit und Informationstechnik) vorgibt. „Bis 2007 gab es für die Polizei keine große Bedrohung durch mobile Endgeräte, denn die bis dahin eingesetzten Betriebssysteme unterstützen die USB-Schnittstelle nicht“, erläutert Michael Kraemer, Kriminaldirektor und Leiter der Abteilung LKA 2 - Information und Kommunikation beim LKA Saarland. Dies sollte sich Anfang 2007 ändern, als eine Migration bei Hardware, Software und vor allem dem Betriebssystem anstand. Durch die flächendeckende Einführung von Windows XP war nun erstmals überall der Zugriff auf USB-Schnittstellen möglich. Damit war eine neue Situation geschaffen.

Während Schnittstellen wie USB, Firewire oder Bluetooth mit jeder Aktualisierung leistungsfähiger wurden, wurde die Kontrollmöglichkeit in der Vergangenheit von den großen Sicherheitsanbietern etwas vernachlässigt. Zahlreiche Studien haben aber belegt, dass nicht verwaltete mobile Speichermedien in kürzester Zeit große Datenmengen aufnehmen und in falsche Hände spielen können. Der weit verbreitete iPod etwa kann ein Datenvolumen (und zwar nicht nur Musikdateien) von bis zu 160 Gigabytes speichern, ausreichend für die meisten Kunden- oder Produktdatenbanken. Folgerichtig verschwinden immer häufiger Daten über diese Schnittstellen und auch der Import von unerwünschter Software und Code nimmt zu.

„Damit es bei uns erst gar nicht zu solchen Problemen kommt, haben wir frühzeitig über professionelles Device-Management nachgedacht“, kommentiert Patrick Stift, der beim LKA Saarland im Bereich Betriebssystem- und Datenbankadministration als Systemadministrator arbeitet und gemeinsam mit den Kollegen die gesamte IT administriert. „Die Polizei als Sicherheitsorganisation will und muss Vorreiter in Sachen Sicherheit sein. Entsprechend müssen wir uns gegen Datendiebstahl wappnen, denn immerhin greifen bei uns mehr als 3.000 Anwender an über 1.200 PCs auf sensible Daten zu.“

Gutes Device-Management muss nicht teuer sein

Gesucht wurde eine Lösung, mit der sich die anschließbaren Endgeräte kontrollieren lassen und mit der man eindeutig festlegen kann, wer, wann, wo, welches mobile Endgerät an welchen PC anschließen darf. Die Zugangsberechtigung sollte über eine „Access-White-List“ erfolgen, in die für jeden Mitarbeiter, PC und seine Schnittstellen die zugelassenen mobilen Endgeräte, basierend auf Hersteller- oder Seriennummer festgelegt werden. Da das LKA Microsofts Active Directory als Verzeichnisdienst zur Verwaltung der Anwender einsetzt, sollte die Lösung diese Plattform unterstützen und zudem revisionssichere Protokolle verwenden. Neben einem hohen Funktionsumfang waren einfache Implementierung, intuitive Bedienung ohne großen Schulungsaufwand, umfassende Kontrolle mittels einer Management-Konsole sowie Änderungen in Echtzeit weitere Auswahlkriterien.

Bei der Suche nach einem entsprechenden Produkt setzte Patrick Stift auf das Internet. Die gefundenen Produkte evaluierte er nach ihrer Funktionsvielfalt und so kamen im Februar 2007 letztlich drei Produkte in die engere Auswahl und wurden intensiven Tests unterzogen. Dabei schnitt devicepro am besten ab, insbesondere was die Themen Steuerung, Funktionsvielfalt und Erweiterbarkeit anging. „Ich habe unserem Management devicepro wegen einer Vielzahl von Pluspunkten vorgeschlagen“, begründet Patrick Stift seine Entscheidung. „Ganz wichtig waren die Funktionsvielfalt und die einfache Bedienbarkeit. Auch die granulare Rechtevergabe ist bei mehr als 3.000 Anwendern ein unverzichtbares Plus“.

Einfache Implementierung und Nutzung

Binnen weniger Wochen fiel die Entscheidung und Anfang März 2007 begann bereits die Implementierung. Diese ist sehr einfach: das Produkt steht nach dem Erwerb als Download zur Verfügung, wird lediglich auf einem Server installiert und liest dann alle notwendigen Informationen über das Netzwerk aus der Active Directory. Die Distribution der Client-Komponente erfolgte über eine bereits vorhandene Softwareverteilungslösung. Aktualisierungen, etwa bei einem Versionswechsel erledigt devicepro automatisch, ohne die Gefahr, dass das Netz überlastet wird oder Benutzer durch die Installation bei ihrer Arbeit gestört werden. „Binnen eines Nachmittages hatten wir das Produkt installiert und die wichtigsten Funktionen aktiviert“, bestätigt auch Patrick Stift das einfache Handling der Lösung.

Als Datenbank konnte eine bereits vorhandene Microsoft SQL ohne Zusatzkosten eingesetzt werden, weitere Software wird nicht benötigt. Verwaltet wird das Produkt durch den Administrator über die Managementkonsole. Die intuitive Bedienung der Konsole stellt sicher, dass quasi jeder Admin sofort mit dem Produkt arbeiten kann und zwar ohne jegliche Schulung. Im ersten Schritt wurden alle Endgeräte mit ihren Schnittstellen automatisch durch devicepro erfasst. Basierend auf diesem Inventar setzte man dann entsprechende Regeln auf, durch die man festlegte, wer, wann, wo, mit welchem Endgerät über welche Schnittstelle kommunizieren darf. Da man nicht alle Endgeräte kannte und das LKA hohe Sicherheitsstandards hat, müssen die Mitarbeiter für jedes Gerät einen Antrag stellen. Der Aufwand auf Mitarbeiterseite ist nicht ganz unbeträchtlich, lohnt sich jedoch, denn neben Sicherheit erhält man so ganz nebenbei auch noch eine aktuelle Übersicht der vorhandenen Devices. Das Eintragen eines neuen Devices geht binnen einer Minute über die Bühne und sämtliche Änderungen, welche in der zentralen Managementkonsole vorgenommen werden, stehen im Netzwerk in Echtzeit sofort zur Verfügung.

Den Datendieben auch künftig einen Schritt voraus

Mittlerweile ist devicepro eine verabschiedete Richtlinie beim LKA Saarland und auf jedem Client installiert. „Unser Ziel, dass ausschließlich autorisierte Benutzer ausdrücklich freigegebene Geräte verwenden, haben wir erreicht“, freut sich Patrick Stift. „LKA-Mitarbeiter können heute ihre autorisierten mobilen Endgeräte bundesweit an ihre PCs anschließen - und trotzdem verfügen wir über höchste Sicherheit.“ Ein weiterer Vorteil von devicepro ist der Umgang mit Ausnahmesituationen. Beispielsweise kommt es recht häufig vor, dass ein externes Endgerät vom Betriebssystem falsch erkannt wird, etwa ein PDA als Festplatte, oder dass Seriennummern mehrfach vergeben wurden, so dass eine automatische Erkennung nicht möglich ist. „Mit der demnächst erscheinenden, neuen Version von devicepro kann ich als Administrator diese falschen Zuordnungen sogar korrigieren und eigene Geräteklassen definieren“, so Patrick Stift

In Zukunft soll das Device-Management dezentral organisiert werden, um die zentralen Administratoren zu entlasten. Technisch sind die Voraussetzungen dafür gegeben, denn devicepro beinhaltet bereits ein entsprechendes Rollen- und Berechtigungsmodell, mit dem für jeden Administrator festgelegt werden kann, was er kontrollieren darf. Auch kann man sich vorstellen, in Zukunft das Thema Verschlüsselung durch das Schwesterprodukt „cryptopro“ abzuwickeln. Ein Umstieg auf diese Lösung hätte den Vorteil, dass man dann sowohl Device Management als auch Dateiverschlüsselung über eine zentrale Managementkonsole steuern könnte.

„Mit devicepro hatten wir das Management der mobilen Endgeräte von Anfang an sicher im Griff“, so das Fazit von Michael Kraemer. „Neben der umfassenden Funktionalität möchte ich vor allem die enge Zusammenarbeit mit dem Hersteller cynapro hervorheben, die weit über den üblichen Support hinausgeht. Unsere Erfahrungen fließen in die nächsten Versionen der Software ein und das gibt uns das gute Gefühl, Datendieben auch künftig immer den entscheidenden Schritt voraus zu sein.“

über cynapspro

Die cynapspro® GmbH ist führender Anbieter im Bereich Data-Loss-Prevention. Das Ettlinger Unternehmen entwickelt Softwarelösungen für den Datenschutz an den Endpunkten von Unternehmensnetzwerken. Damit schließt cynapspro® mit seinen Devicemanagement-, Applikationsmanagement- und Datenverschlüsselungslösungen die Sicherheitslücken die entstehen, wenn im Unternehmen, beispielsweise per USB Sticks, unbefugt Daten vom PC herunter geladen, Notebooks abhanden kommen, Viren und Trojaner jenseits der Firewall eingespielt werden oder unautorisierte Software genutzt wird.

Firmenkontakt:

cynapspro GmbH
Am Hardtwald 1
76275 Ettlingen

Tel.: +49(0)7243 / 945 - 250

Fax: +49(0)7243 / 945 - 100

E-Mail: contact@cynapspro.com

Internet: <http://www.cynapspro.com>