Sichere IT-Umgebung für digitale Tatortfotos

Ein Projektbericht der Bayerischen Polizei

Digitale Fotografie verspricht enorme Kostenvorteile gegenüber der klassischen chemiebasierten Variante. Um dieses Potenzial zu erschließen, ohne auf der IT-Seite Abstriche bei der Sicherheit zu machen, hat die Bayerische Polizei ein flächendeckendes Device-Management eingeführt.

Das Projekt „Digitale Fotografie" (DiFo) der Bayerischen Polizei soll das Einsparpotenzial digitaler Kameras und Arbeitsabläufe für den Polizeidienst erschließen. Die teuren Verfahren der traditionellen Fotografie von Tatorten auf Filmbild-Kameras mit anschließender Negativ- und Bildentwicklung gehören damit, zumindest in Bayern, nun der Vergangenheit an. Kostenvorteile beziehen sich hierbei nicht nur auf die Erstellung der Fotos, sondern wirken sich über die gesamte Lebensspanne und in den definierten Prozessen positiv aus. Die schnelle – wenn erforderlich bundesweite – Verfügbarkeit digitaler Fotos ist gerade im Jahr der Fußball-Weltmeisterschaft ein weiterer wesentlicher Vorzug gegenüber der früheren Vorgehensweise. Bayern ist mit diesem Ansatz Vorreiter und definiert damit Standards, die nicht nur in der Polizeiarbeit, sondern auch in vielen Behörden und Wirtschaftsunternehmen sehr nützlich sein dürften.

Die Einführung von Systemen zur digitalen Fotografie erfordert jedoch naturgemäß die Nutzung von Schnittstellen zu Kameras und Speichermedien an PC-Arbeitsplätzen, die sorgsam zu reglementieren ist, damit keine Einbußen bei der IT-Sicherheit zu beklagen sind. Hier hat sich die Bayerische Polizei für den Einsatz von DeviceWatch (www.devicewatch.de) der Münchner Firma itwatch GmbH entschieden. Der vorliegende Projektbericht schildert die Anforderungen, Entscheidungsgründe und ersten Erfahrungen.

Das DiFo-Projekt ist eng an die flächendeckende Verfügbarkeit des Betriebssystems Microsoft Windows XP gekoppelt, in dem Peripheriegeräte – im Folgenden meist kurz als Geräte oder auch neudeutsch „Devices" bezeichnet – durch Plug&Play sehr einfach eingesetzt werden können. Zur Verbindung von Devices mit dem PC-Arbeitsplatz dienen (ganz allgemein) die Schnittstellen USB, FireWire, PCMCIA, Bluetooth und einige mehr. Mit diesem leichten Zugang zum PC sind natürlich auch Risiken verbunden, unter anderem das Einbringen von Schadsoftware, das unerlaubte Kopieren von Daten oder das Schaffen unerwünschter Netzverbindungen per WLAN oder Bluetooth (vgl. bspw. [1] und [2]).

Derzeit hat die Bayerische Polizei etwa 20 000 PCs im Einsatz; alle Computer wurden 2005 in wenigen Monaten mit Windows XP ausgestattet. Rasch nach seinem Start meldete das zugehörige Projekt auch die Anforderung, digitale Fotoapparate einbinden zu können. Wie sich herausstellte, handelt es sich hierbei um einen Schlüsselfaktor, der bei Roll-out-Vorhaben anderer Behörden häufig vergessen wird. Diese frühzeitige Kommunikation zwi-

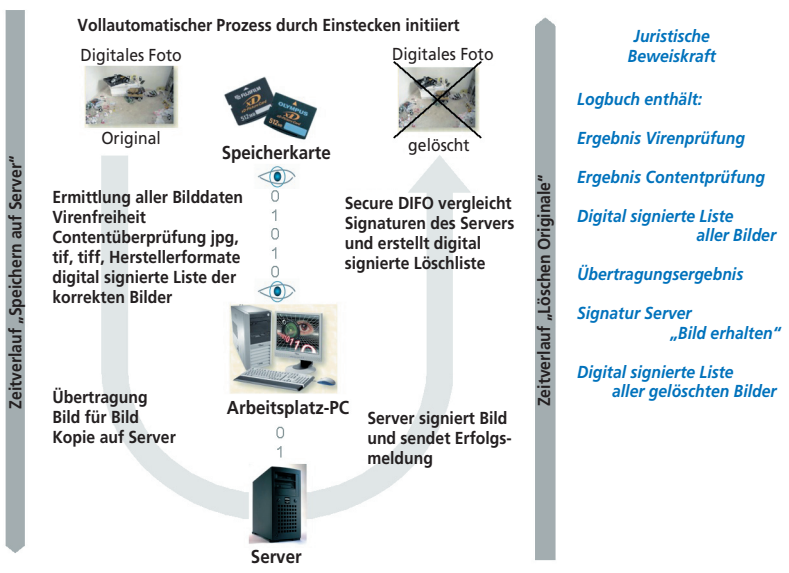

Abbildung 1: Ablauf beim revisionssicheren Auslesen, Speichern und Löschen digitaler Fotos

schen dem Basis-Projekt „Betriebssystem“ und dem Anwendungsprojekt „DiFo“ war entscheidend für ein effizientes Arbeiten.

Bordmittel vs. USB & Co.

Aus Sicht der IT-Plattform – also Betriebssystem und systemnahe Komponenten – ist der sicherste Betrieb dadurch gekennzeichnet, dass alle Schnittstellen mit „Bordmitteln“ abgeschaltet werden. Hierzu stehen Windows Group Policy Objects (kurz GPO), das BIOS sowie lokale Einstellungen zur Verfügung (z. B. Rechte auf bestimmten Registry Keys per Access-Control-Listen). Mit dem Projekt DiFo hatte die Bayerische Polizei aber gerade den Bedarf, die Schnittstellen der Plattform zu *öffnen* – selbstverständlich nur für die vorab definierte Nutzung.

Ein erster Lösungsansatz war es, den ohnehin klar definierten Hardwarebeschaffungsprozess mit zentraler Validierung und Freigabe auch für die Peripheriegeräte zu nutzen. Schnell erkannte man jedoch, dass die Geschwindigkeit, in welcher sich der Markt der Peripheriegeräte verändert, im Rahmen eines zentral gesteuerten Freigabeprozesses nur ungenügend abzubilden ist. Da Kostendruck und Verbesserungen der Flexibilität Hauptgründe für die Realisierung des Projekts DiFo waren, wäre es kontraproduktiv gewesen, realisierbares Einsparpotenzial von vornherein auszugrenzen: Die Kosten digitaler Kameras unterliegen einem stetigen Abwärtstrend, die Modelle werden häufig mit technischen Verbesserungen oder neuen Funktionen unter neuem Namen auf den Markt gebracht, was zeitlich aufwändige, zentrale Validierungsprozesse ad absurdum führt.

Vom Preisdruck im Markt der Peripheriegeräte kann man am besten dann profitieren, wenn für das Management der Devices „schlanke“ Prozesse definiert werden, die ohne großen zeitlichen und personellen Aufwand ablaufen und gegebenenfalls auch einen häufigen Wechsel zu anderen Herstellern oder neuen Gerätetypen unterstützen. Daraus resultierte die Forderung nach einem wirtschaftlichen Life-Cycle-Management für einen potenziell sehr großen Device-„Zoo“ und die effiziente Integration in definierte Prozesse, vor allem zu Beschaffung und Freigabe.

Selbstredend ist der Sicherheitsbedarf bei Polizeibehörden hoch, weswegen Verfahren regelmäßig auch einem „Negativ-Test“ unterzogen werden, der die Funktion einer Teilkomponente infrage stellt und prüft – am besten „in allen Lebenslagen“. Im vorliegenden Fall zeigte sich bei den BIOS-Einstellungen einiger PCs ein Fehlverhalten: Der Plug&Play-Mechanismus im Betriebssystem und das Betriebssystem selbst sind teilweise „stärker“ als das BIOS, sodass eine Sperre von USB-Schnittstellen mit BIOS-Mitteln in bestimmten Fällen nicht mehr greift und der Benutzer dennoch Zugang zu einigen Devices erhält – der Negativ-Test für das Bordmittel BIOS konnte somit nicht als bestanden gelten.

Ein weiteres Problem: BIOS und GPO ermöglichen es nicht, spezifische, durch ihren Namen identifizierte Devices für einzelne Benutzer oder Gruppen freizugeben. Außerdem schützen diese Bordmittel nicht vor Schnittstellen oder Geräteklassen, die zum Roll-out-Zeitpunkt noch nicht bekannt sind. Dadurch entsteht eine permanente Notwendigkeit zur Nachschau.

Verfahren mit ACLs auf einzelne Registry Keys werden überdies schon durch die Treiber einiger Geräte ausgehebelt, die beispielsweise sofort einen neuen Registry-Schlüssel anlegen, wenn sie einen vordefinierten Key nicht mehr lesen können – wenn sie an einer bestimmten Stelle keine Schreibberechtigung haben, suchen sie sich einfach einen anderen Platz.

Speziallösung gefordert

Nach der Analyse aller verfügbaren Bordmittel war damit klar, dass wegen fehlender Flexibilität und limitierter Funktionalität eine andere Lösung gefunden werden musste. Nach einer kurzen Marktsondierung fiel die Entscheidung „Make or Buy“ klar in Richtung „Einkauf“, da der vorgefundene Reifegrad entsprechender marktgängiger Produkte eine Inhouse-Entwicklung nicht rechtfertigt und von anderen Stellen über „Groschengräber“ mit stark wachsenden Kosten bis hin zur Kos-

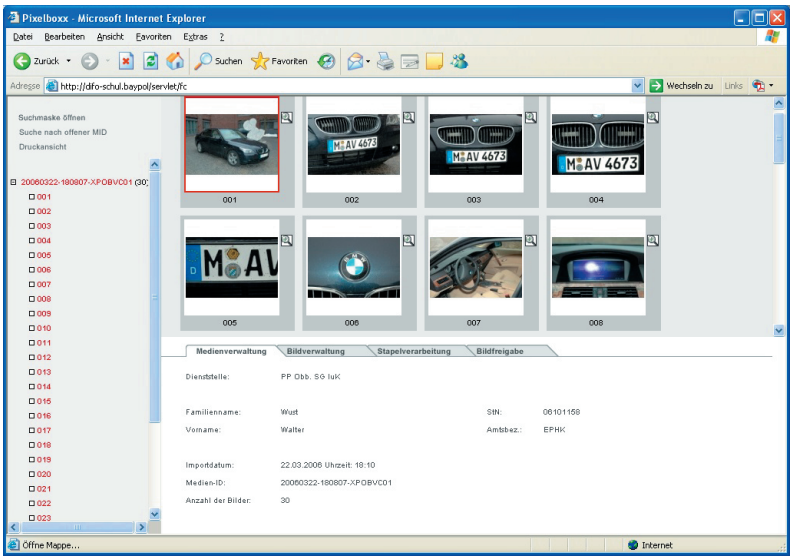

Abbildung 2: Erfasste digitale Fotos werden über eine Client-/Server-Anwendung im Bayerischen Landeskriminalamt verwaltet.

tenexplosion berichtet wurde. Deshalb begann man Ende 2004 mit einer Ausschreibung „sichere Schnittstellen“ ein Werkzeug zu suchen, welches das sichere Management einzelner Devices sowie aller Schnittstellen ermöglicht. Den Zuschlag in dieser Ausschreibung erhielt im ersten Halbjahr 2005 das Produkt DeviceWatch.

DeviceWatch dient dazu, alle Schnittstellen und Peripheriegeräte (auch großer PC-Netze) zentral zu managen – auch für neue, bis dato unbekannte Systeme ist hierfür kein Software-Update erforderlich. Die DeviceWatch DEvCon (Device Event Console) ermöglicht es, auf dezentral auftretende gerätespezifische Ereignisse (z. B. Plug&Play-Fehler, neues Laufwerk, verbotene Netzwerkkarte o. Ä.) individuell zu reagieren und auch eigene Lösungen zu integrieren. Die Konsole umfasst zudem Funktionen zur Inventarisierung peripherer Endgeräte, was überdies – ohne clientseitige Software-Installation – auch durch den DeviceWatch Scanner möglich ist. Nicht zuletzt enthält die Lösung einen Content-Filter mit detailliertem, kundenseitig erweiterbaren Pattern Matching zur syntaktischen und semantischen Kontrolle von Dateiinhalten beim Austausch mit externen Laufwerken. Als weitere Pluspunkte konnte der Anbieter eine branchenübergreifende Marktdurchdringung anführen und durch Referenzinstallationen einen hohen Produktreifegrad belegen.

Parallel zum Management der (zulässigen) Devices als solche blieb noch eine weitere Herausforderung: Ein einmal freigegebenes Gerät, beispielsweise eine Kamera, könnte auch von Berechtigten entweder versehentlich oder sogar absichtlich missbraucht werden. Digitale Kameras sind heutzutage letztlich auch Datenträger mit einem „ganz normalen“ Dateisystem, wodurch einerseits das Risiko eines unerwünschten Exports (Schreiben auf eine Kamera) und zum anderen eines verbotenen Imports entsteht (Lesen von verbotenem Material).

Auch wenn Windows XP ein Flag kennt, mit dem man das Schreiben auf USB-Speichergeräte generell verhindern kann, so ist auch dieses Bordmittel für das DiFo-Projekt unzureichend, da es nur auf USB wirkt, also eingebaute Speicherkartenleser nicht miteinbezieht. Zudem erweist es sich im täglichen Betrieb als sehr lästig: Hier muss beispielsweise ein Administrator, der zum Schreiben berechtigt sein soll, das Flag jedes Mal verändern und er darf vor allem nach der Nutzung das Rücksetzen nicht vergessen. Diese manuelle Aktion ist nicht zumutbar und darüber hinaus äußerst fehleranfällig.

Hinzu kommt ferner, dass einige Standard-Anwendungen beim Öffnen von Fotos kleinere Änderungen an dem genutzten Dateisystem-Ordner vornehmen und bei einem Schreibschutz auf dieses Directory mit undefinierten Fehlern abbrechen. Als endgültiges K.-o.-Kriterium erwies sich bei der Bayerischen Polizei die Einbindung in einen sicheren DiFo-Prozess, der nicht nur zwischen Lesen und Schreiben unterscheidet, sondern der beispielsweise die Aktion „Löschen“ erst nach der Erfüllung bestimmter Bedingungen zulässt.

Sicherer DiFo-Prozess

Innerhalb der Bayerischen Polizei ist definiert, dass ein Tatortfoto erst dann vom Originaldatenträger gelöscht werden darf, wenn bewiesenermaßen eine identische Kopie auf einem dafür vorgesehenen Server angekommen ist. Technisch gesehen müssen die Fotos folgenden Prozess durchlaufen:

_____ Kopieren der Fotos vom Originaldatenträger in eine Quarantänezone und Anlegen von Integritätssignaturen für jedes Foto in einem Protokoll

_____ Prüfung aller Fotos auf Virenfreiheit (Freiheit von sog. Malicious Code) sowie inhaltlicher (semantischer) und syntaktischer Korrektheit: Dabei sind nicht nur die bekannten JPG-Formate EXIF und JFIF zu berücksichtigen, sondern auch die (Kamera-)herstellertypischen Rohformate, die eine höhere Auflösung und damit die Grundvoraussetzung für forensisch detaillierte Analysen bieten.

_____ Nach positiver Prüfung folgt die Übertragung der Fotos auf den Server

_____ Die Rückmeldung des Servers auf einem sicheren Kanal liefert Integritätssignaturen zu jedem einzelnen Foto, die mit jedem Original-Foto verglichen werden. Erst wenn dieser Inhalt korrekt über den sicheren Kanal bestätigt ist, wird ein Löschzertifikat erstellt.

_____ Das Foto wird vom Originaldatenträger gelöscht und das Löschprotokoll archiviert.

Die digitalen Originalbilder (volles Datenvolumen) werden auf einem lokalen File-Server im LAN der erfassenden Dienststelle gespeichert. Ein Vorschau-Bild nebst automatisiert erzeugten Metadaten wird zudem an das Bayerische Landeskriminalamt (BLKA) übertragen, das diese Informationen in einer zentralen Bilddatenbank erfasst und bereitstellt. Die Bildverwaltung übernimmt dabei das Produkt „Pixelboxx“ (vgl. Abb. 2) – das gesamte Verfahren läuft auf einem zentralen Applikationsserver und einem Datenbankserver (mit Oracle 10g als DBMS). Unter bestimmten Voraussetzungen ist zudem vorgesehen, zu netzlastarmen Zeiten auch die voluminösen Vollbilder zu einer übergeordneten Dienststelle zeitversetzt zu übertragen.

Alle einzelnen Schritte und ihre Ergebnisse müssen zudem in einem gemeinsamen Protokoll (Log-

File) revisionssicher hinterlegt werden. Der Investitionsschutz verbietet hier offenkundig proprietäre Lösungen, die nur auf einen (oder einzelne) Kamerahersteller zugeschnitten sind oder bei der Freigabe eines neuen Kameratyps eine Anpassung an der Software benötigen, da der hiermit verbundene Qualitätssicherungsprozess zu teuer und zudem zu langsam wäre, um auf dem schnelllebigen Gerätemarkt geeignet reagieren zu können.

Ergonomie und Kosteneffizienz

Neben der Sicherheit lagen zudem Anforderungen an Ergonomie und kostengünstigen Betrieb im Fokus des DiFo-Projekts. Im Folgenden seien hier stellvertretend nur einige signifikante Eigenschaften aufgeführt:

_____ Der DiFo-Prozess ist automatisiert zu starten, sobald eine Kamera per externer Schnittstelle angeschlossen wird.

_____ Der Benutzer muss über das Fortschreiten des Prozesses permanent informiert bleiben.

_____ Der Anwender muss durch eine abschließende Meldung über den Status und eventuell notwendige Folgeaktivitäten unterrichtet werden; hierbei war es wichtig, eigene Formulierungen einbringen zu können.

_____ Prinzipiell ist eine White-List für Kameras und Flash-Datenträger durchzusetzen, da keine privat erworbenen Datenträger verwendet werden dürfen.

_____ Die Freigabe eines neuen Typs muss im laufenden Betrieb von einer zentralen Stelle für alle Benutzer oder einzelne Benutzer mit minimalem Aufwand (unter fünf Minuten) möglich sein. Dies schließt auch die syntaktische und semantische Prüfung der Bildinhalte mit ein (auch in den jeweiligen Rohdatenformaten).

_____ Eine Prozesseinbindung bei der Beschaffung muss insofern gegeben sein, dass das Plug-in einer verbotenen Kamera den Nutzer sofort mit der Information versorgt, wie er den Beschaffungsvorgang einer freigegebenen Kamera initiiert. Es dürfen hier keine überflüssigen Telefonate entstehen.

_____ Der Life-Cycle der Sicherheitseinstellungen (Security Policy) muss sich in einfacher und revisionssicherer Weise auch in einen Qualitätszyklus mit Test-, Validierungs- und Produktionsumgebung abbilden lassen, ohne die gesamte Infrastruktur zu doppeln.

_____ Wünschenswert ist zudem eine enge Einbindung in den Service-Desk, der über Plug&Play-Fehler am besten in Echtzeit informiert werden sollte.

Fazit

Das DiFo-Projekt hat insgesamt eine sichere Plattform erforderlich gemacht, welche die folgenden abstrakten Anforderungen erfüllt und dabei offen für die Integration eigener Erweiterungen oder Sonderwünsche ist:

_____ detailliertes Logging,

_____ Integration eigener Prozesse (z. B. als Plug-in mit einer Auto-Start-Funktion als Reaktion auf bestimmte Ereignisse wie den Anschluss einer neuen Kamera),

_____ im Produkt vorgesehene Standardprozesse (z. B. Beantragung und Beschaffung sowie Life-Cycle-Management der Security Policies),

_____ Content-Filter mit inhaltlicher Prüfung (semantische und syntaktische Elemente kundenseitig erweiterbar).

Aus projektübergreifender Sicht sind neben den genannten „harten“ Faktoren auch einige „weiche“ Entscheidungsgründe von Bedeutung: Die Auswahl einer neuen tragfähigen IT-Plattform und die darauf aufsetzenden Geschäftsprozesse ist mit hohem Aufwand verbunden und wird deshalb nur in Zeitabständen von fünf bis zehn Jahren erneuert. Die Entscheidung für eine Softwarelösung, die (nur) alle Projektanforderungen sicher und effizient abdeckt, ist deshalb zu kurz gegriffen. Vielmehr müssen die Lösungen für das DiFo-Projekt eine Basis bilden, die auch andere Anforderungen aus dem E-Government für den sicheren und kosteneffizienten Betrieb von Schnittstellen und Geräten erfüllt.

DeviceWatch ist mittlerweile auf allen 20 000 PCs der Bayerischen Polizei im produktiven Einsatz. Es gibt keine offenen Support-Calls und es gab weder während der Validierung noch dem Roll-Out nennenswerte negative Vorkommnisse. Die Lösung hat sich bislang für alle skizzierten Herausforderungen bewährt. ■

Walter Wust (Walter.Wust@Polizei.Bayern.de) ist Leiter Sachgebiet IuK des Polizeipräsidiums Oberbayern.

Text erstmals erschienen in <kes> 2006‘2

Literatur

[1] Peter Scholz, Plug & Plague, Sicherheitsdefizite durch automatische Geräteerkennung, <kes> 2004#1, S. 6

[2] Peter Scholz, Unbekannte Schwachstellen in Hardware und Betriebssystemen, in: Handbuch der Telekommunikation, Wolters Kluwer Verlag, März 2005, ISBN 3-87156-096-0