MSAB

Wie zwei Polizeibehörden im Vereinigten Königreich Effizienz und Kontrolle beim Management digitaler Beweise massiv steigerten

CASE-STUDY

MSAB.com

Marsch 2022

Die Aufgabe

VOR EINIGEN JAHREN haben zwei Polizeibehörden im Vereinigten Königreich ihre Teams für die Digitalforensik aus Kostengründen und zur Effizienzsteigerung zusammengelegt. Das Team bestand aus etwa 200 ausgebildeten Ermittlern, die auf mehrere Standorte verteilt waren. Für Untersuchungen aller Beweise, bei denen digitale Aspekte zu berücksichtigen waren, wurde die Software XRY eingesetzt.

Die Abteilung für Digitalforensik hatte jedoch mit einigen Schwierigkeiten zu kämpfen:

- Es gab Rückstände an auszulesenden und zu analysierenden Mobilgeräten.
- Die für die forensische Extraktion von Mobilgeräten und zum Speichern der Vorgangsdateien verwendeten Computer gerieten permanent an ihre Speicherplatzkapazitäten. In der Folge zögerten die Ermittler häufig, von zu verarbeitenden Telefonen Daten herunterzuladen.
- Da die Computer nicht vernetzt waren, war es schwierig, die Software XRY kontinuierlich auf die neueste Version aktualisieren. Software-Updates wurden an die einzelnen Standorte als DVDs versendet, aber die Updates der Software blieben eine Glückssache.
- Es war schwierig, über alle Standorte hinweg konsistent zu arbeiten und eine einheitliche Qualität zu halten.
- Da es an Anleitung durch die Abteilungsleitung fehlte, wechselten die Nutzer häufig ihre Profile.
- Einzelne Nutzer änderten ihre Kennwörter, was zu Schwierigkeiten bei der Wiederherstellung der Zugangsdaten führte.
- Extrahierte Vorgangsdateien wurden auf DVDs gebrannt und mussten physisch dorthin verbracht werden, wo man die Daten benötigte. Dies erforderte teilweise Fahrzeiten von bis zu 3,5 Stunden, woraus sich „ein Minenfeld an Problemen und dauerhaftes Durcheinander“ ergab.
- „Wir wussten einfach nicht, wer aus welchem Grund Zugang zu den Geräten hatte, wussten nicht, wie oft wie viele Daten heruntergeladen wurden, wo sich diese Daten befanden und wer darauf Zugriff hatte“, fasst der Abteilungsleiter und Analyst für Digitalforensik die Lage zusammen.

„Als ich MSAB Kiosk kennenlernte und erkannte, wie die Software vernetzt arbeiten kann, war ich gleich Feuer und Flamme“, sagt der Abteilungsleiter und Analyst für Digitalforensik. „Aber ich brauchte Jahre, bis das endlich genehmigt wurde.“

Im Vereinigten Königreich müssen alle Digitalforensik-Labore der Polizei zur Gewährleistung von Konsistenz und Qualität ihrer Arbeit ein Qualitätsmanagementsystem nach ISO 17025 einhalten.

Die Änderung des Status-quo: Der Wendepunkt

„Ich argumentierte damit, dass ISO 17025 auch für die Mobilgeräte-Forensik eingeführt werden würde. Wenn wir also dieselben Fähigkeiten auch bei den Ermittlungen vor Ort haben wollten, um auf diese Weise durchgängig gültige Ergebnisse zu erzielen, müssen wir in Zukunft sowieso auf eine vernetzte Infrastruktur zurückgreifen. Warum sollen wir das dann nicht gleich einführen? Das würde uns bei der Einhaltung der ISO 17025 unterstützen.“

„Ich führte aus, dass nach Einführung einer vernetzten Umgebung in jeder Polizeidienststelle ein Mitarbeiter die Daten herunterladen könnte, anstatt dass alle nur an ihren Schreibtischen auf deren Eintreffen warteten. Das Herumgereise und Aktualisieren der Geräte kostete zwei Tage. Diese Zeit könnten wir besser damit verbringen, die Ermittlungsarbeit zu unterstützen.“

„Wir haben rund dreißig Dienststellen, in denen die Leute mit ihrer alltäglichen Arbeit beschäftigt sind. Es kommt also immer wieder vor, dass die Daten vom Telefon eines Verdächtigen heruntergeladen werden, aber der Analyst, der sich damit beschäftigen soll, in einer anderen Station wartet.“

Ein anderer Faktor, der für die Veränderung sprach, war die Übernahme der Datenschutz-Grundverordnung (DSGVO). Dabei geht es um den Schutz von Daten und um die hohen Geldstrafen, die bei Verletzungen vorgesehen sind.

„Es könnte uns, verlören wir die DVD mit den personenbezogenen Daten von jemandem, bis zu eine Million Pfund Strafe kosten."

Was zu tun war: Implementierung

„Nachdem die Genehmigungen erteilt waren, ging es superschnell, alles zu erhalten. Es dauerte ab dem Eingang von ‚Kiosks' lediglich acht Wochen bis zum Go-live." „Es sind überhaupt keine Probleme aufgetreten. Wir mussten wirklich nur den Knopf drücken."

„Der Support durch MSAB war großartig. Es waren ein paar Telefonate erforderlich. Einige Male brauchten wir Unterstützung vor Ort, als es um die Installation und die Tests ging. Diese Arbeiten vor Ort wurden vor dem Go-live erledigt. MSAB hat wirklich den besten Support. Seitdem läuft alles reibungslos."

Kundennutzen

Nachdem die beiden Polizeibehörden die Software XEC Director installiert und alle „Kioske“ verknüpft haben, werden die Dateien mit den extrahierten Daten nun auf den zentralen Server hochgeladen. Es werden also keine Dateien mehr auf DVDs gebrannt, und alle Nutzer haben ihre eigenen Ordner. Es gibt keine Speicherplatzprobleme mehr.

„Die Lösung von MSAB hatte durch Folgendes positive Auswirkungen auf unsere gemeinsamen Kräfte:

- Die Daten stehen beiden Behörden mehr oder weniger sofort zur Verfügung. Wenn wir also, einen Mordfall in einem Bezirk haben und das Ermittlungsteam im anderen, muss niemand mehr auf das Eintreffen der DVDs warten, die dann auch noch kopiert werden müssen. Wir haben jetzt einen Fast-Echtzeit-Zugriff auf die Daten.
- Außerdem lassen sich alle Updates der Software XRY mithilfe von XEC Director verwalten. Es wird also keine Zeit mehr für das Herumfahren verschwendet, und wir sparen auch sehr viel Geld. Bislang waren die Kioske außergewöhnlich stabil, und ihre Auto-Detect-Funktion ist hervorragend.
- Die Nutzer müssen sich nicht mehr mit XRY beschäftigen, nachdem sie die Kioske erhalten haben. Da der Workflow sie Schritt für Schritt anleitet, scheuen sie sich nicht länger die Software auch einzusetzen. Eher sind alle von der Schnelligkeit beeindruckt. Niemand muss sich länger darum sorgen, dass das System abstürzt oder der Speicherplatz knapp wird.
- Dank der Steuerungsmöglichkeiten fühlen sich die Nutzer unterstützt. Software-Updates lassen sich einfacher umsetzen. Bei Problemen können die Vorgesetzten den Nutzern auch aus der Ferne helfen. Als Vorgesetzter kann ich erkennen, wie viele Daten wir erzeugen. Die Protokollfunktion finde ich klasse. Da ich eindeutige und konsistente Protokolle für die Führungskräfte erstellen kann, werden wir auch weitere Kioske erwerben.

– Zusammengefasst: Ich habe jetzt eine zentral konfigurierte und gesteuerte Umgebung, bei der alle Daten zentral gespeichert werden. Unsere Nutzer können die neuesten Versionen von XRY und der Software XAMN für die Mobilgeräte-Forensik einsetzen. Ein weiterer großer Vorteil ist, dass die Führungskräfte die Vorteile erkannt haben.“

„Die Umstellung auf MSAB Kiosk und auf eine Netzwerklösung war die beste Entscheidung, die wir treffen konnten. Heutzutage können wir zum Beispiel hoch gefährdete Opfer häuslicher Gewalt wesentlich besser schützen. Früher wurde durch die Abhängigkeit vom Labor das Verfahren mindestens einen Monat verzögert. Mithilfe von Kiosk können wir die Verdächtigen in der Vernehmung direkt mit den extrahierten Beweisen konfrontieren, und eine Anklage kann innerhalb der ersten acht Stunden erhoben werden.“

– Abteilungsleiter und Analyst für Digitalforensik