Étude de cas : améliorer la qualité et le flux des renseignements numériques essentiels dans la lutte contre le terrorisme et réduire les coûts d'exploitation

Fallstudie: Verbesserung der Qualität und Übermittlung von wichtigen digitalen Informationen bei der Terrorismusbekämpfung und Reduzierung der Betriebskosten

Avancées majeures

En 2010, une agence gouvernementale de collecte de renseignements pour la lutte contre le terrorisme, basée aux principaux points de passage frontaliers et dotée de forces spéciales antiterroristes, a eu une mission extrêmement importante, mais – ironiquement – avec un potentiel d'analyse criminalistique numérique limité. Le personnel n'a procédé qu'à la lecture des cartes SIM avec un matériel inadéquat et désuet ; ce qui a entraîné une collecte limitée de renseignements. Il a fallu trois à quatre semaines à une équipe d'analyse centrale pour récupérer les données du site de téléchargement.

Mais l'agence a pris conscience de l'enjeu et a commencé à apporter des changements. Au cours d'une période de sept ans, l'investissement continu en équipement d'analyse criminalistique mobile et l'interconnexion de réseaux ont apporté des améliorations importantes. Une quantité considérable de renseignements est désormais recueillie et les équipes centrales reçoivent ces informations en quelques heures.

Errungenschaft

Im Jahr 2010 hatte eine staatliche geheimdienstliche Behörde zur Terrorismusbekämpfung, die an wichtigen Grenzübergangspunkten saß und spezielle Befugnisse für die Terrorismusbekämpfung hatte, einen äußerst wichtigen Auftrag, aber – ironischerweise – nur begrenzte Möglichkeiten, was die digitale Forensik anging. Das Personal konnte lediglich SIM-Karten lesen – und das mit schlechter, veralteter Ausrüstung, was die Möglichkeit der Erfassung von Daten stark einschränkte. Die Übermittlung der gesammelten Daten von dem Standort, an dem sie heruntergeladen wurden, an ein zentrales Analyseteam dauerte drei bis vier Wochen.

Doch die Behörde stellte sich der Herausforderung und begann, einiges zu verändern. Über einen Zeitraum von sieben Jahren wurde kontinuierlich in Ausrüstung für Mobilgeräte-Forensik und in eine bessere Vernetzung investiert. Dies führte zu signifikanten Verbesserungen. Jetzt werden große Mengen an Informationen gesammelt, die innerhalb weniger Stunden an die zentralen Teams weitergeleitet werden.

FRANÇAIS

Problème/enjeu

En raison de l'utilisation accrue d'appareils mobiles, les agences de renseignements étaient désireuses de puiser dans cette précieuse source de données. Elles avaient le pouvoir légal d'accéder aux données d'appareils mobiles appartenant à des voyageurs internationaux qui cherchaient à entrer sur le territoire. Mais en 2010, elles ne possédaient pas l'équipement approprié pour le faire. La pression financière était également omniprésente. Il fallait donc une solution avec un bon rapport qualité-prix.

L'agence a lancé une nouvelle initiative pour moderniser son équipement, sa formation et son infrastructure afin, non seulement de capturer les données, mais aussi de s'assurer que les renseignements obtenus parviennent rapidement à ceux qui en avaient besoin. Ce potentiel devait être développé sur plusieurs années, car l'argent était toujours à court.

Au début du projet, cela prenait plus de deux semaines pour envoyer des données limitées à un concentrateur, mais elles n'étaient pas vraiment partagées avec une base de données centrale. Si des analystes voulaient les données, ils devaient les demander expressément et le transfert des données était lent. Les renseignements essentiels n'arrivaient donc pas là où on en avait le plus besoin, et même lorsque les informations étaient transmises, cela pouvait prendre jusqu'à quatre semaines entre la capture et l'analyse des données.

Solution

En 2010, une équipe de deux agents a constitué la division de criminalistique numérique et rédigé une analyse de rentabilité montrant à quel point il était possible de recueillir plus de renseignements essentiels à l'aide de la technologie d'analyse criminalistique mobile actuelle. Plus précisément, ils ont recommandé les kits MSAB Office, considérés comme la meilleure technologie. Au départ, six kits Office Logical ont été utilisés à des endroits clés, et deux kits Office Physical ont été achetés pour les agents spécialisés ayant reçu une formation

DEUTSCH

Problem/Herausforderung

Aufgrund der zunehmenden Nutzung von Mobilgeräten war es ein wichtiges Ziel der Geheimdienste, in diese wertvolle Datenquelle einzudringen. Sie waren gesetzlich berechtigt, auf Mobilgeräte von einreisewilligen Personen zuzugreifen, verfügten im Jahr 2010 jedoch nicht über die dazu erforderliche Ausrüstung. Die finanziellen Mittel waren ebenfalls begrenzt, so dass jede Lösung ihr Geld auch wert sein musste.

Die Behörde begann also, ihre Ausrüstung, Ausbildung und Infrastruktur zu modernisieren, damit die Daten nicht nur erfasst würden, sondern auch schnell dorthin gelangen würden, wo sie gebraucht werden. Da das Geld stets knapp war, nahm dieser Modernisierungsprozess einige Jahre in Anspruch.

Zu Beginn des Projekts dauerte es über zwei Wochen, bis die Daten bei einer zentralen Sammelstelle ankamen. Darüber hinaus wurden sie nicht in einer zentralen Datenbank gespeichert. Wenn Analysten die Daten benötigten, mussten sie sie speziell anfordern – und die dann folgende Datenübermittlung war langsam. All dies bedeutete, dass wichtige Informationen nicht dort ankamen, wo sie benötigt wurden, und selbst wenn sie übermittelt wurden, vergingen zwischen Erfassung und Analyse teilweise bis zu vier Wochen.

Lösung

Im Jahr 2010 gründeten zwei Ermittler die Einheit für digitale Forensik und demonstrierten, wie sehr viel mehr wichtige Informationen mit moderner Technik für Mobilgeräte-Forensik gesammelt werden könnten. Insbesondere empfahlen sie MSAB Office-Kits als beste Technologie. Zunächst wurden sechs Office Logical-Kits an den wichtigsten Standorten eingeführt und zwei Office Physical-Kits für speziell ausgebildete Ermittler erworben. Anschließend erhielten alle 190 Ermittler an den Standorten der Behörde eine Grundlagenschulung zur Durchführung einfacher logischer Extraktionen.

FRANÇAIS

supplémentaire. Ensuite, les 190 officiers déployés sur les sites de l'agence ont reçu une formation de base afin d'effectuer les téléchargements logiques de base, c'est-à-dire le travail à volume élevé.

En 2013, un agent d'encadrement a été engagé pour examiner le travail, optimiser et simplifier les processus. Le nombre d'utilisateurs de base a été réduit de 190 à 50 ; ce qui s'est traduit par des économies grâce à la réduction du temps de formation et en raison de la perte d'heures de travail par les agents.

L'argent économisé a été investi en engageant deux officiers supplémentaires dans la division spécialisée ; ce qui leur a permis d'acquérir les compétences et le matériel nécessaires pour s'acquitter de leur tâche. Ces deux nouveaux officiers ont suivi des cours de formation intermédiaire et avancée MSAB, ainsi que d'autres cours généraux d'analyse criminalistique mobile. Cela a permis de s'assurer que, dans les cas hautement prioritaires, les agents spécialisés effectueraient les téléchargements, et qu'il y aurait suffisamment d'agents formés.

Il a encore fallu veiller à ce que les données parviennent rapidement là où on en avait besoin. Le transport manuel des données de chaque site vers le concentrateur coûtait environ 33 000 livres sterling par an.

Les 33 000 livres sterling ont en grande partie servi à rémunérer les officiers pour leur temps passé à transporter les données. Parmi les autres aspects négatifs du transport des données, mentionnons le risque de cogner le disque dur et d'endommager les données, et le fait que pendant le transfert, l'agent était absent de son poste et incapable de s'acquitter de sa tâche principale.

Une autre méthode aurait consister à transporter les données à l'aide d'un réseau de données ; ce qui aurait coûté environ 20 000 livres sterling, y compris un lecteur NAS de 10 To, et les travaux à effectuer. Le réseau de messagerie interne de l'agence ne pouvait pas faire face à la taille des téléchargements : taille limite des fichiers de 5 Mo.

DEUTSCH

2013 wurde die Arbeit durch einen beaufsichtigenden Ermittler überprüft, der auch die Prozesse verbesserte und rationalisierte. Die Anzahl der Grundanwender wurde von 190 auf 50 reduziert, was zu Ersparnissen durch weniger Schulungen und weniger „verlorene" Arbeitsstunden der Ermittler führte.

Das eingesparte Geld wurde in die Erweiterung der Anzahl Spezialisten von zwei auf vier Ermittler investiert, die entsprechend geschult wurden und die erforderliche Ausrüstung erhielten. Sie absolvierten MSAB-Schulungen für Fortgeschrittene und für Experten sowie weitere allgemeine Schulungen zur Mobilgeräte-Forensik. Hierdurch wurde gewährleistet, dass die Extraktionen in Fällen von hoher Priorität von Spezialisten durchgeführt werden und dass genügend speziell hierfür ausgebildete Ermittler zur Verfügung stehen.

Aber das Problem der langsamen Datenübermittlung war hiermit noch nicht gelöst. Die Kosten für den manuellen Transport der Daten von allen Standorten zur zentralen Sammelstelle betrugen ungefähr £33.000 im Jahr.

Der Großteil dieser £33.000 entstand dadurch, dass die Daten durch Ermittler persönlich überbracht wurden. Andere Nachteile des Datenübermittlungsprozesses waren zum Beispiel, dass die Daten auf einer Festplatte durch einen Stoß oder Sturz beschädigt werden konnten und dass der jeweilige Ermittler während der Überbringung der Daten nicht an seinem Platz war und seinen eigentlichen Aufgaben nicht nachkommen konnte.

Eine Alternative war, die Daten über ein Datennetz zu übertragen, das ca. £20.000 kosten würde, einschließlich eines 10-TB-NAS-Laufwerks und der Einrichtung des Netzwerks. Die Kapazität des internen E-Mail-Systems der Behörde reichte für die Menge der heruntergeladenen Daten nicht aus – die Dateigröße war auf 5 MB beschränkt.

FRANÇAIS

Le câble à fibres optiques avait déjà été posé pour un autre projet ; ce qui a permis d'éliminer ce coût. Le chiffrement logiciel a été installé sur les bureaux de sorte que les données soient chiffrées pendant la transmission.

La simple interconnexion de réseaux a permis d'économiser 15 000 livres sterling par an et de réduire à zéro le temps consacré au transfert des données du site de téléchargement vers le concentrateur, car les appareils ont été téléchargés directement sur le disque NAS. La sécurité du transfert a été augmentée et l'intégrité des données est garantie.

Ce n'était cependant que la moitié de la solution, car les données devaient encore aller du concentrateur vers la base de données centrale.

Pour ce faire, une solution cloud computing a été mise en œuvre, car il y avait une plus grande zone géographique à couvrir, et l'utilisation du « stockage cloud » comme un conduit a éliminé le besoin de câblage terrestre coûteux.

Cela a un coût, mais il a été en partie compensé par les économies déjà identifiées par l'interconnexion des bureaux aux réseaux. Le chiffrement au niveau matériel a été utilisé de part et d'autre pour assurer la sécurité et l'intégrité du transfert.

Ainsi, à la fin de 2014, il existait une solution réseau sécurisée permettant de s'assurer que les données collectées par les agents au moment de la capture puissent être transmises en quelques heures aux analystes du centre.

En 2015, avec l'arrivée imminente de la norme de conformité ISO 17025, la décision a été prise de mettre à niveau les kits Office Logical pour passer aux MSAB Logical Kiosks.

Beaucoup de travail de « réflexion » à été ainsi enlevé aux utilisateurs de base, leur permettant de se concentrer sur l'obtention de bons téléchargements. Le flux de travail a été revu pour répondre aux besoins de la division et les Kiosks connectés au réseau. Le chiffrement logiciel a été

DEUTSCH

Glasfaserkabel waren bereits für ein anderes Projekt verlegt worden, so dass hierfür keine weiteren Kosten anfielen. Für die Datenübertragung wurde Softwareverschlüsselung auf allen Desktopcomputern eingerichtet.

Allein durch die Vernetzung sparte die Behörde jährlich £15.000. Darüber hinaus wurde die für die Datenübertragung vom jeweiligen Standort an die zentrale Sammelstelle erforderliche Zeit auf Null reduziert, da die Daten direkt auf das NAS-Laufwerk heruntergeladen wurden, die Übertragungssicherheit wurde verbessert und die Datenintegrität wird gewährleistet.

Doch das war nur die halbe Lösung, da die Daten ja noch von der zentralen Sammelstelle in die zentrale Datenbank gelangen mussten.

Hierfür wurde eine Cloud-Lösung implementiert, da ein größerer geografischer Bereich abgedeckt werden musste und durch die Speicherung in der Cloud die kostenintensive Übertragung per Kabel wegfiel.

Natürlich fielen hierfür zunächst einmal Kosten an – die aber durch die Einsparungen, die durch die Vernetzung der Computer erzielt wurden, teilweise ausgeglichen wurden. Um die Sicherheit und die Integrität des Transfers zu gewährleisten, wurde Hardwareverschlüsselung an beiden Enden eingeführt.

So hatte man Ende 2014 eine sichere Netzwerklösung, über die die von den Ermittlern am jeweiligen Standort erfassten Daten innerhalb weniger Stunden an die Analysten übermittelt werden konnten.

Im Hinblick auf die Einführung der Norm ISO 17025 wurde im Jahr 2015 die Entscheidung getroffen, die Office Logical-Kits zu MSAB Logical-Kiosks aufzurüsten.

Dies bedeutete, dass den Grundanwendern eine ganze Menge „Denkarbeit" abgenommen wurde und dass sie sich darauf konzentrieren konnten, hochwertige Extraktionen zu erhalten. Der Arbeitsablauf wurde an die Bedürfnisse der Einheit angepasst und die Kiosks wurden an das Netzwerk angeschlossen. Des weiteren

FRANÇAIS

ajouté ; ce qui a assuré la sécurité de la transmission des données.

L'avantage supplémentaire était que l'utilisation de Kiosks a permis de répondre aux exigences de la norme ISO 17025. Le Kiosk est conçu pour ne faire qu'une seule chose : un téléchargement XRY. Grâce à l'ajout de caméras, l'agence disposait désormais d'un produit de renseignement complet d'analyse criminalistique, d'une qualité probante et capable d'être livré aux analystes en quelques heures.

Après un court laps de temps, il a été décidé d'ajouter XEC Director, un autre produit de MSAB, pour aider à gérer le réseau de Kiosks, faire des rapports et exécuter d'autres fonctions de gestion centralisée.

Tous les trois ans, les besoins et les outils requis par la division sont analysés. La solution MSAB continue de recevoir des notes excellentes en comparaison avec d'autres outils utilisés par l'agence, en tenant compte du coût, de l'exhaustivité des données capturées et de la rapidité d'acquisition.

Conclusion

L'agence gouvernementale de collecte de renseignements pour la lutte contre le terrorisme dispose désormais d'un système de capture numérique entièrement interconnecté, hautement performant et fiable sur le plan criminalistique, garantissant que les données vitales ne prennent que quelques heures pour aller de la capture à l'analyse et traverser de vastes zones géographiques. Ce potentiel continue d'être utile pour détecter régulièrement les menaces et les suspects terroristes découverts grâce aux preuves numériques.

DEUTSCH

wurde eine Softwareverschlüsselung eingerichtet, um die Datensicherheit bei der Übertragung zu gewährleisten.

Ein weiterer Vorteil war, dass mit der Einführung der Kiosks ein großer Schritt in Richtung Erfüllung der Norm ISO 17025 getan wurde. Denn die Kiosks haben nur eine einzige Aufgabe: die Durchführung von XRY-Extraktionen. Durch die zusätzliche Nutzung von Kameras verfügte die Behörde nun über ein Produkt zur Erfassung vollständiger, beweiskräftiger forensischer Daten, die innerhalb weniger Stunden an die Analysten übermittelt werden konnten.

Nach kurzer Zeit wurde beschlossen, auch XEC Director einzuführen, ein anderes MSAB-Produkt, um die Verwaltung des Kiosk-Netzwerks, die Erstellung von Berichten und andere zentrale Verwaltungsaufgaben zu erleichtern.

Alle drei Jahre werden die Bedürfnisse der Einheit und die erforderlichen Tools überprüft. Im Vergleich zu den anderen von der Behörde eingesetzten Tools erzielt die MSAB-Lösung im Hinblick auf Kosten, Vollständigkeit der erfassten Daten und Geschwindigkeit der Datenerfassung weiterhin hervorragende Bewertungsergebnisse.

Schlussfolgerung

Die Behörde zur Terrorismusbekämpfung verfügt nun über ein voll vernetztes, hochleistungsfähiges, forensisch zuverlässiges digitales Datenerfassungssystem, mit dem die erfassten Daten innerhalb von nur wenigen Stunden über große geografische Entfernungen zur Analyse übermittelt werden können. Dieses System trägt regelmäßig zur Aufdeckung von terroristischen Bedrohungen und Verdächtigen durch digitale Beweise bei.