Anwenderbericht

TNS Infratest schützt heikle Daten abseits der IT-Abteilung

Wer mit sensiblen Personendaten arbeitet, unterliegt strengen Sicherheitsrichtlinien. TNS Infratest generiert jährlich Hunderttausende dieser Daten und ist seit 2013 eines der wenigen ISO 27001 zertifizierten Unternehmen in Deutschland. Um ihren oft global agierenden Kunden noch mehr Sicherheit garantieren zu können, vertrauen die Münchner Markt- und Innovationsforscher auf das Verschlüsselungstool HiCrypt™.

Es begann bei TNS Infratest mit der Rundfunk-Hörerforschung und entwickelte sich im Laufe der letzten 60 Jahre zu einem der renommiertesten Institute für wissenschaftliche und wirtschaftliche Markt- und Meinungsforschung. Jährlich werden 300.000 Interviews in verschiedenen Formen zu ganz unterschiedlichen Themen erhoben. Somit generieren die Münchner riesige Volumina an Daten, die politische und soziale Erkenntnisse sowie die Weiterentwicklung von Produkten und Dienstleistungen beeinflussen. Zahlreiche Ministerien, Behörden sowie national und global tätige Unternehmen verlassen sich auf die Expertise TNS Infratest.

Neben allgemeinen Daten arbeitet TNS Infratest vor allem mit sensiblen Informationen, ganz gleich ob auf Kunden- oder auf Teilnehmerseite. Daher ist die Datensicherheit ein wichtiges Thema. Ende 2013 erhielt TNS Infratest aufgrund seines Informationssicherheitsmanagements die ISO 27001 Zertifizierung des TÜV Süd. Doch das reicht einzelnen Kunden nicht aus. Zu groß ist die Sorge vor unautorisiertem Datenzugriff. Vor allem Unternehmen, die an innovativen Themen, wie Energieoptimierung oder Automobilentwicklung arbeiten, fürchten den unerlaubten Zugriff oder Verlust ihrer Datenschätze.

Besonders deutlich wurde dies im Herbst 2013: Für die Zusammenarbeit mit einem großen Automotive-Kunden musste TNS Infratest Sicherheitsanforderungen erfüllen, die das bisherige, eh schon hohe Maß, noch deutlich überschritten. Gefunden haben die Security-Experten bei TNS Infratest schließlich HiCrypt™, eine Netzlaufwerk-Verschlüsselung der Chemnitzer digitronic computersysteme gmbh.

Unabhängigkeit von der IT-Abteilung entschied die Evaluation

Vor der Entscheidung für HiCrypt™ hat TNS Infratest den Markt für Verschlüsselungslösungen gründlich geprüft. Die Komplexität der Anwendung als auch die Lizenzkosten waren zwei mitschwingende Faktoren, doch als K.O.-Kriterium für die Angebote der großen internationalen Hersteller entpuppte sich ein selten beachtetes Feature: der von der IT-Abteilung vollkommen unabhängige Betrieb der Sicherheitslösung.

„Was nützt mir eine ausgefeilte Sicherheit gegen Bedrohungen von Außen, wenn zig interne IT-Mitarbeiter potenziellen Zugang zu den hochsensiblen Daten unserer Kunden haben?“, kommentiert Dirk Wocke, Informationssicherheitsbeauftragter bei TNS Infratest. „Für die eigenen Leute können wir zwar die Hand ins Feuer legen, aber das hilft ab einem gewissen Geheimhaltungslevel in der Argumentation mit dem Kunden nicht mehr weiter. Deshalb war es für uns ausschlaggebend, dass HiCrypt™ die eigenverantwortliche Nutzung der Software durch den Fachbereich ermöglicht – ganz ohne Zutun der IT.“, erklärt Wocke weiter.

Aufgrund der Fokussierung auf die wesentlichen Funktionen benötigt das Verschlüsselungs-Tool keine spezielle IT-Infrastruktur, so dass ein von der IT-Abteilung losgelöstes Rollout im entsprechenden Fachbereich von TNS Infratest realisiert werden konnte.

„Wir konnten die Implementierung selbstständig ohne zusätzliche Hilfe von digitronic, unserer inhouse IT-Abteilung oder Dritten durchführen. Das hat uns enorme Kosten gespart. Auch eine individuelle Anpassung war nicht notwendig. Es funktionierte nahezu out-of-the-box", sagt Sicherheitsexperte Wocke. Die Implementierung des Verschlüsselungssystems brauchte circa fünf Manntage. Dazu kamen knapp zwei Tage für die Schulung aller Anwender. „HiCrypt™ soll in der Basisversion einfach nur die Netzlaufwerke verschlüsseln. Und das extrem zuverlässig und quasi ohne Möglichkeit der Fehlbedienung. Wir finden es beispielhaft, wie schnell die Forschungsexperten bei TNS Infratest HiCrypt™ in ihre gewohnte Arbeit integrieren konnten", sagt Matthias Kirchhoff, Geschäftsführer der digitronic computersysteme GmbH.

Ausführliche Testphase und Zusatzfeatures

Nach der kurzen Schulung begann bei TNS Infratest sofort ein dreiwöchiger Test. „Da wir ein bestehendes Backup-Konzept besitzen, musste die Verschlüsselungssoftware unbedingt auch mit diesem kompatibel sein. Das hat HiCrypt™ mit Bravour erfüllt", betont Wocke. In dieser Phase wurde die Wiederherstellung aus Archiven ausgiebig getestet. HiCrypt™s Pluspunkt: Das Tool verschlüsselt ausschließlich Inhalte. Ordnerstrukturen und Dateinamen bleiben erhalten. Inkrementelle und differentielle Datensicherungen werden somit vollständig unterstützt.

Aktuell nutzen 20 TNS Infratest Mitarbeiter aus der Münchner Zentrale das Tool der Chemnitzer. Die einmaligen Lizenzkosten beliefen sich auf circa 3.000 Euro. Die Nutzergruppe ist vorrangig mit Kunden aus dem Automotive-Markt beschäftigt. Dirk Wocke erklärt: „Da HiCrypt™ eine integrierte Benutzerverwaltung hat, kann sich der Fachbereich selbstständig um die Zugriffsverwaltung kümmern und ist nicht auf die Hilfe der IT-Abteilung angewiesen. Das bringt uns im Produktivbetrieb erhebliche Zeit- und Kostenersparnisse."

Einziges Manko bei der Einführung von HiCrypt™ war die damals fehlende 2-Faktor-Authentifizierung. Diese musste zunächst durch ein separates Tool gelöst werden, wurde jedoch schnell von digitronic® durch die Markteinführung von HiCrypt™ 2.0 und USB Smartcard Token Unterstützung gelöst. „Die für uns bisher wichtigste Erweiterung der HiCrypt™-Nutzung ist die Einführung der 2-Faktor-Authentifizierung. Damit konnten wir einen etwas umständlichen Workaround ablösen und alles in einer Lösung konsolidieren", berichtet der Informationssicherheitsbeauftragte der TNS Infratest.

Sicherheit ist kein Hype-Thema

Durch die Erweiterung um die 2-Faktor-Authentifikation und die einfach Handhabung hat sich HiCrypt™ in die alltägliche Arbeit der TNS Infratest eingegliedert.
Damit das Nutzungserlebnis weiterhin so positiv ausfällt wie bisher, haben die Münchner Meinungsforscher einen Software Pflegevertrag für HiCrypt™ abgeschlossen. Somit werden sie weiterhin mit wichtigen Aktualisierungen und Erweiterungen versorgt und profitieren im Ernstfall vom Support der Chemnitzer Entwickler.

„Wir sind mit HiCrypt™ sehr zufrieden und gehen von einer Ausweitung der Zusammenarbeit bei überaus sicherheitssensiblen Projekten aus. Der Bedarf dürfte in Zukunft stark steigen.“, fasst Dirk Wocke zusammen. Und schon sind die Mitarbeiter der TNS Infratest wieder in die Tiefen von Wahlprognosen, Marktforschung und Innovationsberatung abgetaucht.

HiCrypt™-Funktionen

Verschlüsselung von Netzlaufwerken

HiCrypt™ ermöglicht die Verschlüsselung von Netzwerklaufwerken. Die Ver- und Entschlüsselung findet auf dem Client statt, somit wird ein sicherer Datenaustausch zwischen Client und Server gewährleistet. Folgende Algorithmen werden zur Verschlüsselung genutzt: AES (256 Bit), Blowfish (448 Bit) und IDEA (128 Bit).

Schlüsselalleinbesitz-Garantie

HiCrypt™ garantiert seinen Nutzern die alleinige Kontrolle über die Schlüsselinformationen zu den verschlüsselten Daten. Mit dem Zero Knowledge-Prinzip gewährleistet der Hersteller, keinerlei Zugriff auf die Daten zu haben.

Gemeinsames Arbeiten

Im Vergleich zu herkömmlichen Container-Verschlüsselungen bietet HiCrypt die Möglichkeit eines gemeinsamen Zugriffs und ist somit für die sichere Teamarbeit geeignet.

Zentrale Benutzerverwaltung

HiCrypt™ besitzt eine integrierte Nutzerverwaltung, die losgelöst von der IT-Abteilung konfiguriert werden kann. Die Benutzerverwaltung lässt sich unabhängig von lokalen oder Domänen-Benutzerkonten einsetzen.

Zugriff auf Cloud-Speicher

HiCrypt™ unterstützt, neben Standard-Windows-Freigaben, auch Online-Festplatten, die sich als Netzlaufwerke einbinden lassen. Somit können Cloud-Dienste genutzt werden, um verschlüsselte Dateien auszutauschen. Zudem unterstützt HiCrypt Terminalserver-Umgebungen und eignet sich somit für viele Varianten von Desktop as a Service-Anwendungen.

Disaster Recovery

HiCrypt™ bietet verschiedene Möglichkeiten havarierte verschlüsselte Daten wiederherzustellen.

Unterstützung von SmartCards

HiCrypt™ unterstützt aktuell alle SmartCard- oder USB-SmartCard-Tokens, die vom SafeSign Identity Client verwendet werden. Zudem können unternehmensweite Kennwortrichtlinien mit HiCrypt abgebildet werden.

Unterstützung von Rollout-Strategien

Durch die einfache Installation kann HiCrypt™ problemlos in jede Rollout-Strategie integriert werden. Es wird keine extra IT-Infrastruktur benötigt.

Unterstützung von Microsoft Betriebssystemen

HiCrypt™ unterstützt die Desktop- und Server-Varianten aus dem Hause Microsoft in der 32- und 64-Bit Version.

Apps für mobile Entschlüsselung

HiCrypt™ bietet eine App für iOS und Android Smartphones und Pads. Somit lassen sich auch unterwegs die verschlüsselten Daten entschlüsseln.

Kontakt

TNS Infratest
Dirk Wocke
Informationssicherheitsbeauftragter
Telefon: +49 (0) 89 5600-2185
E-Mail: dirk.wocke@tns-infratest.com

digitronic computersysteme GmbH
Peter Liebing
Oberfrohnaer Straße 62
09117 Chemnitz
Telefon: +49 (0) 371 81539-0
Telefax: +49 (0) 371 81539-900
E-Mail: marketing@digitronic.net
Internet: www.digitronic.net,
www.hicrypt.com