

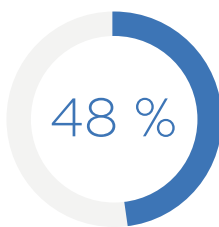


WHITEPAPER

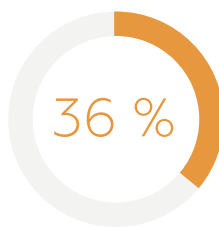
SECURE IT ASSET DISPOSITION (ITAD) SCHÜTZT VOR DATENPANNEN UND IMAGESCHÄDEN

Wenn Unternehmen ihre IT-Assets nicht sorgfältig nachverfolgen und entsorgen, setzen sie sich großen Risiken aus - es drohen unter anderem Datenpannen, Bußgelder und auch eine Schädigung ihres Rufs. Ein ITAD-Programm zur sicheren Entsorgung von IT-Assets kann helfen, die Gefahr von Datenpannen zu verringern. Bob Johnson (CEO von i-Sigma) und Brooks Hoffman (Principal of Secure IT Asset Disposition bei Iron Mountain) trafen sich zu einem Gespräch über Missverständnisse beim Thema Secure ITAD, Business-Cases aus der Branche und die sich verändernde Landschaft der IT-Asset-Disposition. Sie tauschten sich darüber aus, wie Kunden ihr Unternehmen positionieren können, um solche Risiken zu vermeiden.

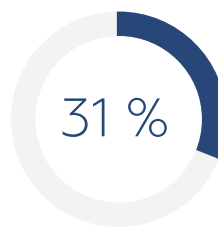
WICHTIGSTE THEMEN BEI ITAD



DATENSICHERHEIT



EINHALTEN GESETZLICHER VORSCHRIFTEN



SICHERE NACHWEISKETTE

QUELLE: IDG & Iron Mountain Research 2019

DREI GRÜNDE FÜR ITAD:



VORSCHRIFTEN
EINHALTEN



NEGATIVE
SCHLAGZEILEN
VERMEIDEN



GEISTIGES
EIGENTUM
SCHÜTZEN

Als CEO von i-SIGMA, einem Branchenverband mit weltweit über 1.700 Mitgliedern aus den Bereichen Datensicherheit und Informationsmanagement, hat Bob Johnson über 40 Jahre Erfahrung mit Datenschutz und Compliance - und kennt viele Szenarien aus erster Hand. In erster Linie müssen Unternehmen die Entsorgung ihrer IT-Assets wichtig genug nehmen, damit die verschiedenen Datenschutzrichtlinien eingehalten werden können. „Sie sind rechtlich verpflichtet, die personenbezogenen Daten Ihrer Mitarbeiter und Kunden zu schützen“, so Johnson. Gemäß DSGVO (Datenschutz-Grundverordnung) müssen Unternehmen auf Nachfrage Auskunft dazu geben, welche Daten sie gespeichert haben, und diese Daten auf Verlangen löschen. In Südafrika gilt seit dem 1. Juli 2021 mit dem Protection of Personal Information Act (POPIA) eine ganz ähnliche Regel, und auch in den USA gibt es verschiedene nationale und regionale Gesetze, mit denen persönliche Daten geschützt werden. Ein weiterer Grund, warum Sie sich über die IT-Asset Disposition Gedanken machen sollten: Wenn Sie die Daten Ihrer Mitarbeiter und Kunden nicht schützen, drohen negative Schlagzeilen, die teure, rufschädigende Folgen haben können.

Probleme geben.“ Es gibt noch einen dritten Grund, warum eine sichere Entsorgung von IT-Assets so wichtig ist: Unternehmen, die geistiges Eigentum besitzen, denken oft nur daran, die personenbezogenen Daten zu schützen, wie es das Gesetz vorschreibt, vergessen dabei aber, dass eine falsche Entsorgung auch ihr geistiges Eigentum in Gefahr bringt. Wenn Unternehmen nach einem Datendiebstahl nicht nachweisen können, dass sie die vertraulichen Informationen - zum Beispiel Geschäftsgeheimnisse - adäquat geschützt haben, sind diese Informationen möglicherweise für immer verloren. „Dann verlieren Sie Ihr Recht an diesen Daten“, so Johnson. „Sie müssen zeigen, dass Sie die ganze Zeit auf ausreichend Sicherheit geachtet haben.“

Der richtige Fokus

Einige Unternehmen kennen diese Bedrohungen, doch viele denken noch nicht daran. Sie konzentrieren sich nur auf die Vernichtung von Daten - obwohl sie auch für die Vernichtung ihrer IT-Assets einen umfassenden Prozess mit soliden Richtlinien brauchen. „Manchmal konzentrieren sich Unternehmen auf einzelne Bäume statt auf den ganzen Wald“, so Hoffman. „Sie legen den Fokus fälschlicherweise auf Methoden zur Datenvernichtung und auf einzelne Spezifikationen, statt ein allgemeines Framework für ihr ITAD-Programm aufzustellen, zu dem gut dokumentierte Richtlinien und Prozesse gehören.“

„DIE ENTSORGUNG VON IT-ASSETS SOLLTE NIEMAND AUF DIE LEICHTE SCHULTER NEHMEN.“

BOB JOHNSON, CEO BEI I-SIGMA

So musste beispielsweise in 2020 eine internationale Investment-Bank hunderttausende Kunden darüber informieren, dass deren Informationen nicht ordnungsgemäß geschützt waren - und zwar, weil das Unternehmen vier Jahre zuvor seine IT-Geräte nicht richtig entsorgt hatte. „Sie mussten allein deshalb über die Panne informieren, weil die theoretische Möglichkeit bestand, dass die Assets einem Sicherheitsrisiko ausgesetzt waren“, erklärt Johnson. Die Folge? Bußgelder in Höhe von 60 Millionen US-Dollar. „Wenn Datenschutzverletzungen gemeldet werden müssen, wird das sehr teuer.“ Bei verloren gegangenen IT-Assets, so Johnson, ist jedes einzelne Gerät „eine potenzielle Zeitbombe. Die Pflicht zur Meldung von Datenschutzverletzungen verjährt nicht. Deshalb sollte niemand die Entsorgung von IT-Geräten auf die leichte Schulter nehmen. Ich würde sogar sagen: Wenn man sie nicht ernst genug nimmt, wird es unter Garantie

Unternehmen versteifen sich oft zu sehr auf Vernichtungsmethoden - auf eine externe oder vor Ort eingesetzte Wiping-Software, die Vernichtung bestimmter Medientypen oder die sogenannte Entmagnetisierung zum Löschen der Daten auf magnetischen Datenträgern. Andere Unternehmen entwickeln auch detaillierte Richtlinien dazu, wie klein Medien geschreddert werden müssen, weil sie glauben, dass es schwieriger wird, Daten wiederherzustellen, wenn die Medien nur klein genug zerhäckselt wurden. „Das geht an der Sache vorbei“, so Hoffman. Stattdessen müssen die Verantwortlichen darauf achten, dass sie den Status ihrer datentragenden Assets über den gesamten Lebenszyklus nachverfolgen können. „Das bedeutet: vom Einkauf über die gesamte Nutzungsdauer bis hin zur endgültigen Entsorgung.“ Dieser ganzheitliche Ansatz, der sich „von der Wiege bis zum Grab“ erstreckt, ist bei der Entwicklung eines Entsorgungsprogramms für IT-Assets besonders wichtig. Da sind sich Hoffman und Johnson einig.

Welche Lösung gibt es?

Auch wenn die Geschäftsführung in Entscheidungen zur IT Asset Disposition nicht direkt einbezogen wird, sollte sie trotzdem wissen, welche Risiken es gibt und wie diese sich verringern lassen. Dabei hilft es, „von der Wiege bis zum Grab“ zu denken und ein solides

Entsorgungsprogramm zu entwickeln. Die richtige IT Asset Disposition sollte als eine Investition in Datensicherheit und Umweltschutz gesehen werden und nicht als reine Müllentsorgung, die nur Kosten verursacht.

1

Sensible Daten ermitteln

Ermitteln Sie systematisch, auf welchen IT Assets im Unternehmen sensible Daten gespeichert werden und wo sich diese befinden. Üblicherweise denkt man bei datentragenden Assets erst einmal an Laptops, PCs und Server, doch es gibt auch andere.

„Daten liegen oft auch auf anderen Geräten, die wir erst einmal vergessen“, so Hoffmann. Dazu gehören zum Beispiel medizinische Geräte oder sogar Kopiergeräte. „Man braucht wirklich gute Systeme, um zu verstehen, wo die Assets sind und welche Daten darauf gespeichert wurden.“

2

Konsistente Richtlinien und Prozesse entwickeln

Führungskräfte aus IT und Fachabteilungen sollten außerdem sicherstellen, dass im gesamten Unternehmen konsistente Richtlinien und Prozesse gelten - und dass diese auch eingehalten werden. Es hilft nichts, wenn die Regeln irgendwo in einem Ordner im Regal stehen: Die Angestellten müssen sie kennen und befolgen, insbesondere in großen Unternehmen mit verschiedenen Standorten. Eine richtige Schulung ist wichtig.

„Alle im Unternehmen müssen die Richtlinien und Prozesse kennen“, so Hoffman. Es muss Möglichkeiten geben, die Einhaltung von Regeln zu überwachen, und im Falle einer Missachtung sollte auch mit Konsequenzen gearbeitet werden. „Denn wenn es keine Folgen hat, halten sich die Leute meist nicht an die Prozesse. Dann entstehen Unregelmäßigkeiten und unübersichtliche Einzelsysteme.“

3

Auf eine sichere Nachweiskette achten

Achten Sie auf eine sichere Nachweiskette und die Art der Daten, denn es gibt nicht den einen Ansatz, der für alle Prozesse und Datenbereinigungsmethoden passt.

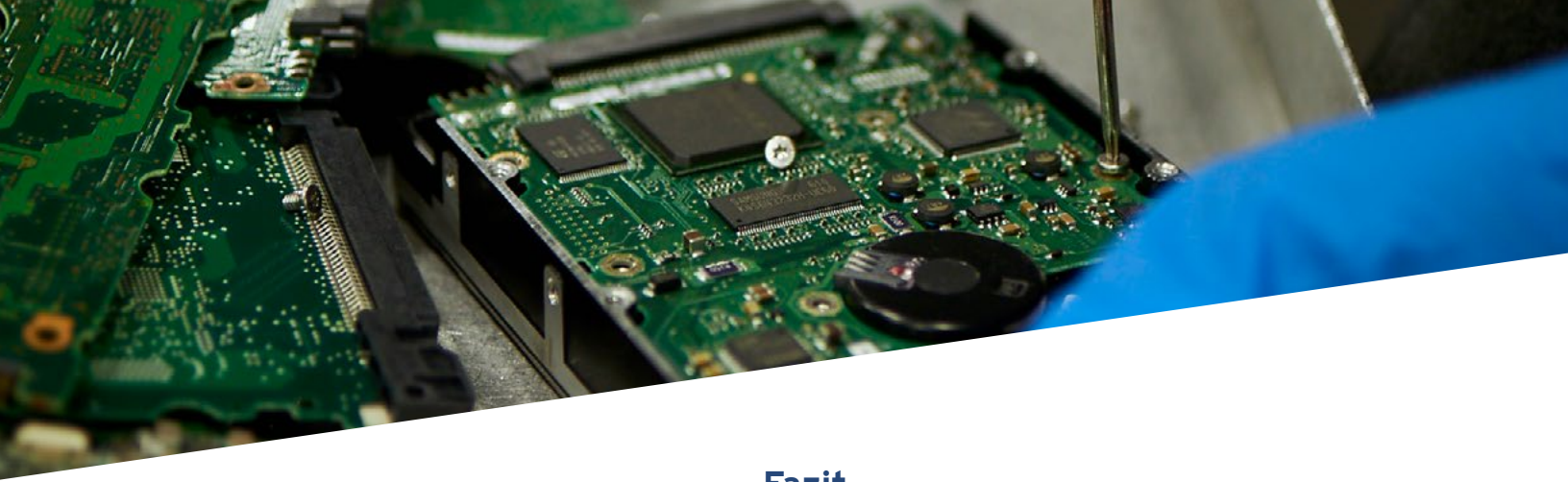
Anders ausgedrückt: Handelt es sich um sensible oder unbedenkliche Daten? So können vertrauliche Daten zum Beispiel schon vor Ort vernichtet werden, damit es während des Transports nicht zu Pannen kommt. Weniger sensible Daten wie Zeitpläne oder Adressen können extern gelöscht werden, solange eine sichere Nachweiskette zwischen den Büros und dem Ort der endgültigen Vernichtung besteht.

4

Lieferanten sorgfältig auswählen

Um Angreifern keine Chance zu geben, sollte Ihr Unternehmen seine Lieferanten sorgfältig auswählen und sie als strategische Partner betrachten. Suchen Sie für die IT Asset Disposition nach vertrauenswürdigen Anbietern, die alle Richtlinien und bewährten Verfahrensweisen der Branche einhalten.

Dabei können Sie in einem ersten wichtigen Schritt auf anerkannte Zertifizierungen für die Datenvernichtung achten, wie zum Beispiel die von i-Sigma. Andere relevante Zertifizierungen für die Entsorgung von IT-Assets sind e-Stewards und R2. Ihre Aufgabe als Führungskraft ist es, bei der Auswahl der Anbieter einen eigenen Due-Diligence-Prozess durchzuführen.



„Es reicht nicht, sich nur die Zertifizierung anzusehen“, so Hoffman. „Manchmal lesen wir von zwielichtigen Firmen, die Elektroschrott ins Ausland verschiffen oder auf einer Deponie entsorgen. Das kann zu Datenpannen und Umweltverschmutzung führen. Auch hier ist es wichtig, vertrauenswürdige Partner auszuwählen. Überprüfen Sie sie unbedingt selbst.“ Due Diligence umfasst in diesen Fällen beispielsweise einen Besuch vor Ort und eine Überprüfung der Richtlinien und Prozesse sowie der vorhandenen Kundenreferenzen.

Fazit

Führungskräfte spielen im Unternehmen eine wichtige Rolle bei der Entwicklung einer umfassenden und sicheren Strategie für die sichere IT Asset Disposition (Secure ITAD). Indem Sie in ein gut durchdachtes Programm investieren und es selbst mitgestalten, schützen Sie Ihr Unternehmen vor teuren Datenpannen, hohen Bußgeldern und einer möglichen Rufschädigung. „Für ein erfolgreiches Programm ist es wichtig, zu verstehen, welche Art von Daten Sie haben, wie sensibel sie sind, wo sie sich befinden - und dass Richtlinien und Prozesse konsequent umgesetzt werden“, sagt Hoffman. In unserem heutigen Umfeld, fügt Johnson hinzu, führt es garantiert zu Problemen, wenn Sie versuchen, die sichere Entsorgung von IT-Assets zu umgehen. „Das ist nur eine Frage der Zeit.“



0800 408 0000 | [IRONMOUNTAIN.DE](https://www.ironmountain.de)

0800 00 24 24 | [IRONMOUNTAIN.CH](https://www.ironmountain.ch)

+43 (0) 2287 30 544 | [IRONMOUNTAIN.CO.AT](https://www.ironmountain.co.at)

ÜBER IRON MOUNTAIN

Iron Mountain ist der weltweit führende Anbieter von innovativen Archiv- und Informationsmanagement-Services. Das 1951 gegründete Unternehmen archiviert und schützt Milliarden wertvoller Vermögenswerte, von geschäftskritischen Dokumenten über hochsensiblen Daten bis hin zu kulturellen und historischen Artefakten. Auf Iron Mountain vertrauen mehr als 225.000 Unternehmen weltweit. Mit seinem breiten Dienstleistungsspektrum, das vom Informationsmanagement über die Unterstützung bei der digitalen Transformation, Rechenzentren, sichere Archivierung und Vernichtung bis hin zur Kunstarchivierung und -logistik reicht, hilft Iron Mountain Unternehmen, Licht ins Dunkel ihrer Daten zu bringen. So können sie den Wert ihrer gespeicherten und archivierten digitalen und physischen Dokumente, Daten, und Informationen schnell und sicher erschließen und gleichzeitig sicherstellen, dass sie ihre Umweltziele erreichen.