CIO FROM IDG SPONSORED CONTENT

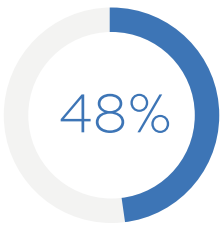
WHITEPAPER

IT-APPARATUUR VEILIG AFVOEREN IS CRUCIAAL OM DATALEKKEN EN IMAGOSCHADE TE VOORKOMEN

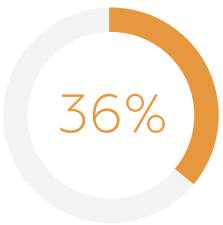
Bedrijven die hun IT-apparaten niet op de goede manier afvoeren lopen allerlei risico's, zoals datalekken, boetes en imagoschade. Maar een vast proces voor de veilige verwijdering van IT-apparatuur (Secure IT Asset Disposition) kan de kans op een datalek verkleinen.

Bob Johnson, CEO van i-Sigma, en Brooks Hoffman, directeur van Secure IT Asset Disposition (SITAD) bij Iron Mountain, doken in dit onderwerp. Ze bespraken misvattingen over SITAD, voorbeelden uit de praktijk, het veranderende landschap en hoe organisaties hun beveiligingsrisico's kunnen beperken.

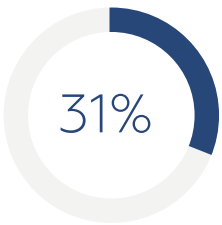
GROOTSTE ZORGEN OVER ITAD



INFORMATIEBEVEILIGING



VOLDOEN AAN REGELGEVING



VEILIGE BEWAKINGSKETEN

BRON: IDG & Iron Mountain Research 2019

IRON MOUNTAIN®

3 redenen waarom ITAD belangrijk is

REGELGEVING

GEEN IMAGOSCHADE

BESCHERMING INTELLECTUEEL EIGENDOM

Bob Johnson is CEO van i-SIGMA, de non-profit brancheorganisatie die wereldwijd meer dan 1.700 locaties in gegevensbeveiliging en informatiebeheer vertegenwoordigt. Hij heeft meer dan 40 jaar ervaring op het gebied van gegevensbescherming en compliance en maakte vele scenario's mee.

In de eerste plaats moeten organisaties over de hele wereld prioriteit geven aan het afvoeren van IT-apparatuur, zodat er aan alle regelgeving rond gegevensbescherming wordt voldaan. "Wettelijk gezien moet je de persoonlijke gegevens van je werknemers en klanten beschermen", zei Johnson.

Dankzij de General Data Protection Regulation (GDPR) kunnen mensen opvragen welke informatie bedrijven over hen hebben verzameld en hun gegevens laten verwijderen. Sinds 1 juli 2021 bevat de Protection of Personal Information Act (POPIA) in Zuid-Afrika soortgelijke regels. In de VS gelden voor bedrijven staats- en federale wetten om de persoonsgegevens van inwoners te beschermen.

Een andere reden om de afvoer van IT-appratuur te prioriteren: als de gegevens van werknemers en klanten niet worden beschermd, kan dat een bedrijf dure en vernietigende krantenkoppen opleveren.

Een derde reden om aandacht te besteden aan de veilige verwijdering van IT-apparaten is de bescherming van intellectueel eigendom. Bedrijven die zich alleen concentreren op de persoonsgegevens die ze volgens de wet moeten beschermen, vergeten soms dat onjuiste verwijdering ook hun intellectueel eigendom in gevaar brengt.

Als bedrijven niet kunnen aantonen dat ze bedrijfseigen informatie beschermden, zoals een handelsgeheim, hebben ze misschien niet langer de rechten op die informatie. "Ze kunnen letterlijk hun recht verliezen om die informatie te beschermen. Ze moeten echt laten zien dat ze de gegevens altijd al beveiligden", zei Johnson.

Welke focus er nodig is

Hoewel sommige bedrijven zich bewust zijn van de risico's, focussen veel van hen zich alleen op gegevensvernietiging. In plaats daarvan kunnen ze beter een uitgebreid kader en beleid voor de veilige verwijdering van IT-apparaten maken.

"Soms richten organisaties zich op de bomen in plaats van op het bos", zei Hoffman. "Ze richten zich ten onrechte op datavernietiging en individuele specificaties, in plaats van een algemeen kader te creëren voor de vernietiging van hun apparaten, inclusief een goed gedocumenteerde reeks beleidslijnen en procedures."

Bedrijven kunnen zich te veel fixeren op vernietigingsmethoden, zoals het wissen via software, op locatie of extern; het vernietigen van media;

"IT-APPARATEN AFVOEREN IS NIET IETS OM TE NEGEREN."
BOB JOHNSON, CEO VAN I-SIGMA

Laatst moest bijvoorbeeld een grote internationale investeringsbank, die niet wist hoe ze 4 jaar geleden hun apparaten hadden weggegooid, honderdduizenden klanten laten weten dat hun gegevens misschien waren gelekt.

"Ze moesten de inbreuk melden omdat er een kans was dat de gegevens risico liepen", zei Johnson. De bank kreeg een boete van 60 miljoen dollar. "Meldingen van inbreuken zijn erg duur."

Johnson zei dat ieder missend IT-apparaat een potentiële tijdbom is. "Er is geen verjaringstermijn voor het melden van inbreuken. Het afvoeren van IT-appraten is niet iets om te negeren. Ik durf zelfs te zeggen dat wanneer het wel wordt genegeerd, dan ontstaat er een probleem."

of degaussen, waarbij een magnetisch veld de data kapot maakt. Sommige organisaties maken ook een beleid voor de grootte van de snippers na vernietiging. Ze gaan ervan uit dat hoe kleiner de snippers zijn, hoe moeilijker gegevens kunnen worden teruggehaald.

"Dit slaat de plank volledig mis", aldus Hoffman. In plaats daarvan moeten leiders de status van hun gegevensdragers gedurende de hele levensduur kunnen volgen. "Dat wil zeggen vanaf de aanschaf, tijdens het gebruik, tot aan de uiteindelijke vernietiging."

Volgens zowel Hoffman als Johnson is deze zogenaamde cradle-to-grave-benadering cruciaal bij het creëren van een ITAD-beleid.

Wat is de oplossing?

Directieleden zijn misschien niet direct betrokken bij beslissingen over de verwijdering van IT-apparaten, maar ze kunnen wel veel doen om de risico's die ermee gepaard gaan te begrijpen en te verminderen. Onder meer door te helpen bij het invoeren van de cradle-to-grave-aanpak en degelijke verwijderingsprocedures. IT-apparaten veilig verwijderen moet worden gezien als een investering in informatiebeveiliging en duurzaamheid in plaats van als een afvalkostenpost.

1 Identificeer de gevoelige gegevens

Focus op systemen en ontdek welke apparaten gevoelige gegevens bevatten én waar deze datadragers zich bevinden. Er wordt vaak gedacht aan laptops, pc's en servers, maar er is nog veel meer cruciale apparatuur.

"Er zitten gegevens in apparaten waar je misschien niet meteen aan denkt, zoals medische testapparatuur of zelfs kopieermachines", zei Hoffman. "Je moet echt een goed systeem hebben om te begrijpen waar de apparaten zijn en welke gevoelige gegevens erop staan."

2 Zorg voor consistente procedures

IT- en bedrijfsleiders moeten een consistent beleid en vaste procedures implementeren en erop toezien dat die worden nageleefd. Sommige organisaties hebben al zo'n map met richtlijnen liggen, maar alle werknemers moeten de regels kennen én volgen, vooral in grote organisaties met meerdere vestigingen. Medewerkers opleiden is dus cruciaal.

"Het is belangrijk dat iedereen in de organisatie begrijpt wat het beleid en de procedures zijn", aldus Hoffman. Er moet een manier zijn om te controleren of werknemers zich inderdaad aan de regels houden én er moeten consequenties volgen na niet-naleving. "Want als er geen gevolgen zijn, zullen mensen de procedures niet volgen en krijg je alsnog een zeer gedecentraliseerd systeem."

3 Focus op een veilige bewakingsketen

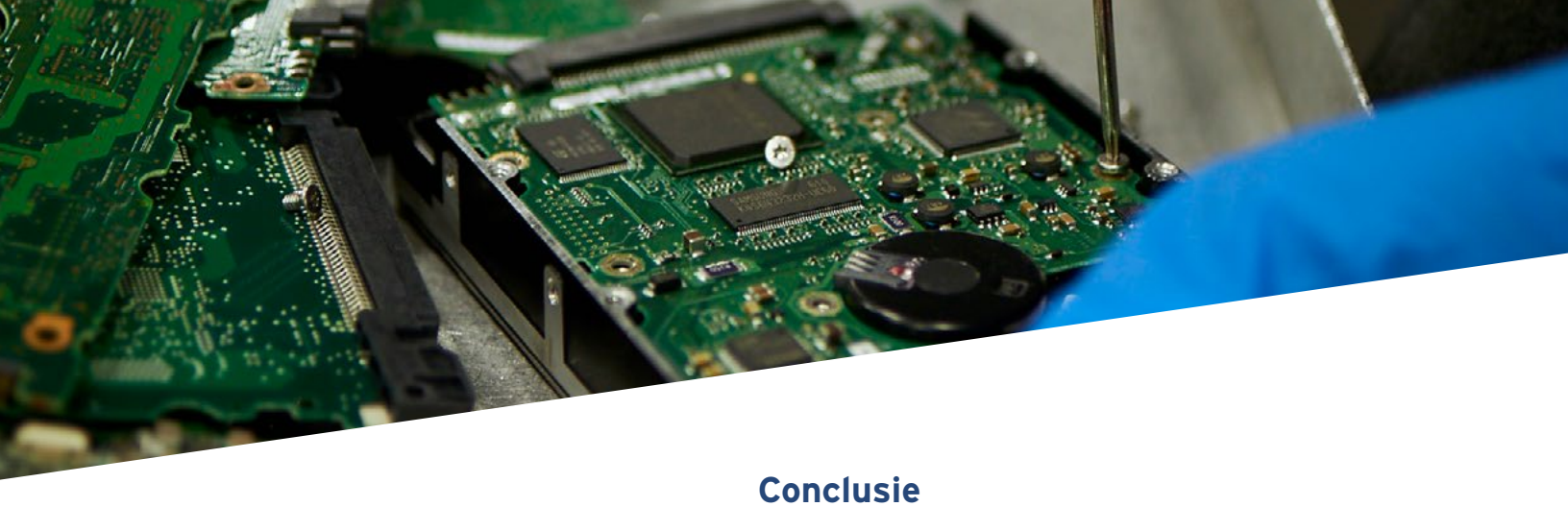
Ga voor op een veilige bewakingsketen en let op de aard van de gegevens, in plaats van alle data op dezelfde manier te vernietigen.

Leiders moeten beoordelen of gegevens gevoelig of routinematig zijn. Vertrouwelijke gegevens kunnen ter plaatse worden vernietigd om inbreuken tijdens de overdracht te voorkomen. Routinematige, minder gevoelige gegevens, zoals planningen of adressen, kunnen best extern worden vernietigd, zolang er maar een veilige bewakingsketen is tussen de locatie en de uiteindelijke verwerkingslocatie.

4 Kies leveranciers met zorg

Om risico's te vermijden moeten leiders goed op zoek gaan naar strategische partners, in plaats van alleen leveranciers. Partners die voldoen aan alle regelgeving en die van de hoed en de rand weten als het op de verwijdering van IT-apparatuur aankomt.

Certificeringen specifiek voor gegevensvernietiging, zoals die van i-Sigma, zijn een handig eerste selectiecriterium. Ook de R2-normen zijn een voorbeeld van een relevante certificering. Maar leiders moeten ook hun eigen research doen bij het kiezen van een passende leverancier. Denk aan het bezoeken van de faciliteiten van potentiële partners en het controleren van hun beleid, procedures en klantreferenties.



"Het is niet genoeg om alleen maar naar certificeringen te kijken", zei Hoffman. "Wij kennen genoeg verhalen over louche bedrijven die e-waste naar het buitenland verscheepten of het ergens hebben gestort, en dat kan leiden tot datalekken en milieuovertredingen. Het is dus belangrijk om zelf betrouwbare partners te kiezen wanneer je van IT-apparatuur af wilt."

Conclusie

Leiders spelen een integrale rol bij het opzetten van een complete strategie voor het veilig verwijderen van IT-apparatuur. Door te investeren in een goed doordacht proces kunnen zij hun bedrijf beschermen tegen kostbare datalekken, boetes en mogelijke imagoschade.

"Inzicht in de aard van de gegevens, hoe gevoelig ze zijn, waar ze zich bevinden, en het consequent volgen van beleid en procedures zijn echt de sleutel tot een succesvolle aanpak", zei Hoffman.

Johnson voegde nog toe: "Als er in de huidige situatie geen aandacht wordt besteed aan het veilig vernietigen van IT-apparatuur, zal dat uiteindelijk een probleem worden. Dat is een kwestie van tijd."

IRON MOUNTAIN®

0800 272 44 33 | IRONMOUNTAIN.NL

OVER IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM), opgericht in 1951, is wereldwijd marktleider op het gebied van opslag- en informatiebeheerdiensten. Vertrouwd door meer dan 220.000 organisaties over de hele wereld en met een netwerk van meer dan 85 miljoen vierkante meter in meer dan 1.400 vestigingen in meer dan 50 landen, bewaart en beschermt Iron Mountain miljarden informatiedragers en documenten, waaronder bedrijfskritische informatie, zeer gevoelige gegevens en culturele en historische artefacten. Iron Mountain biedt oplossingen voor onder meer veilige opslag, informatiebeheer, digitale transformatie, veilige vernietiging en datacenters, kunstopslag en logistiek, en cloud-diensten. Iron Mountain helpt organisaties om kosten en risico's te verlagen, te voldoen aan wet- en regelgeving, te herstellen van calamiteiten en een meer digitale manier van werken mogelijk te maken.