CIO Od IDG TREŚCI SPONSOROWANE

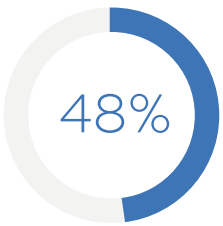
WHITE PAPER

BEZPIECZNA UTYLIZACJA ZASOBÓW IT JEST KLUCZOWA, ABY ZAPOBIEGAĆ NARUSZENIOM DANYCH I CHRONIĆ REPUTACJĘ

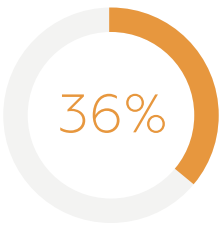
Firmy, które nie śledzą i nie utylizują swoich urządzeń IT we właściwy sposób, stoją w obliczu szeregu poważnych zagrożeń, w tym naruszenia danych, grzywien i potencjalnego uszczerbku na reputacji firmy.

Bezpieczny program utylizacji zasobów IT może pomóc w ograniczeniu możliwości naruszenia bezpieczeństwa danych. Bob Johnson (dyrektor generalny i-Sigma) i Brooks Hoffman (dyrektor ds. bezpiecznej utylizacji zasobów IT w Iron Mountain) przedstawili błędne wyobrażenia na temat utylizacji zasobów IT, rzeczywiste przykłady biznesowe, zmieniające się okoliczności utylizacji urządzeń oraz sposób pozycjonowania organizacji w celu złagodzenia zagrożeń bezpieczeństwa danych.

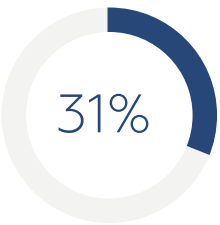
NAJWAŻNIEJSZE ASPEKTY UTYLIZACJI URZĄDZEŃ IT



OCHRONA DANYCH



ZGODNOŚĆ Z WYMOGAMI REGULATORÓW



BEZPIECZNY ŁAŃCUCH NADZORU (CHAIN OF CUSTODY)

ŹRÓDŁO: IDG i Iron Mountain Research 2019

IRON MOUNTAIN®

3 powody, dla których utylizacja zasobów IT jest ważna:

REGULACJE

OCHRONA PRZED UTRATĄ WIZERUNKU

OCHRONA WŁASNOŚCI INTELEKTUALNEJ

Johnson ma ponad 40-letnie doświadczenie w ochronie danych i przestrzeganiu zgodności z przepisami (compliance). Jako dyrektor generalny i-SIGMA, stowarzyszenia handlowego non-profit reprezentującego ponad 1700 członków zajmujących się bezpieczeństwem danych i zarządzaniem informacjami. Wiele rzeczy widział na własne oczy.

Przede wszystkim firmy na całym świecie muszą traktować priorytetowo utylizację urządzeń elektronicznych, aby zapewnić zgodność z różnymi wymaganiami w zakresie ochrony danych. „Zgodnie z prawem należy chronić dane osobowe pracowników i klientów, z którymi się współpracuje" — powiedział Johnson.

Ogólne rozporządzenie o ochronie danych (RODO) pozwala na sprawdzenie jakie dane na nasz temat zostały zebrane przez różne firmy i jeśli chcemy usunięcia ich. W Republice Południowej Afryki ustawa o ochronie danych osobowych (POPIA), która weszła w życie 1 lipca 2021 r., określa podobne zasady. W Stanach Zjednoczonych firmy podlegają przepisom nakazującym ochronę danych osobowych zarówno na poziomie stanowym, jak i federalnym.

Kolejny powód, dla którego należy traktować priorytetowo utylizację zasobów IT to fakt, że: brak ochrony danych pracowników i klientów może skutkować opiniami, które negatywnie wpłyną na wizerunek firmy.

Trzecim powodem, dla którego należy zadbać o bezpieczną utylizację zasobów IT jest ochrona własności intelektualnej.

Firmy, które koncentrują się wyłącznie na danych osobowych, do ochrony których są zobowiązane przez prawo, mogą nie zdawać sobie sprawy, że niewłaściwe zarządzanie wycofanym sprzętem IT może stanowić zagrożenie również dla ochrony własności intelektualnej.

Jeśli organizacja nie jest w stanie udowodnić, że chroniła informacje zastrzeżone, takie jak tajemnica handlowa, może utracić prawa do tych informacji. „Dosłownie może stracić prawo do ich ochrony" – powiedział Johnson. „Musi udowodnić, że przez cały czas odpowiednio dbała o bezpieczeństwo".

Na czym musisz się skoncentrować

Niektóre firmy są świadome tych zagrożeń, wiele z nich traktuje priorytetowo metody niszczenia danych. Jednak to nie wystarcza. Powinny tworzyć kompleksowe, bezpieczne ramy utylizacji zasobów IT, oparte na przemyślanych zasadach.

„Czasami firmy skupiają się na drzewach, a nie na całym lesie" – powiedział Hoffman. „Błędnie skupiają się na metodach niszczenia danych i indywidualnych specyfikacjach, zamiast na tworzeniu ogólnych ram dla programu utylizacji zasobów IT, opartego na dobrze udokumentowanym zestawie zasad i procedur".

„UTYLIZACJI ZASOBÓW NIE MOŻNA IGNOROWAĆ".

BOB JOHNSON, DYREKTOR GENERALNY I-SIGMA

Na przykład w zeszłym roku duży międzynarodowy bank inwestycyjny, nieświadomy tego, w jaki sposób pozbył się swoich zasobów IT cztery lata wcześniej, musiał powiadomić setki tysięcy klientów, że bezpieczeństwo ich danych zostało naruszone.

„Musieli powiadomić o naruszeniu bezpieczeństwa danych, bo istniało duże prawdopodobieństwo, że dane faktycznie były zagrożone" – powiedział Johnson. Bank dostał karę w wysokości 60 milionów dolarów. „Powiadomienia o naruszeniach są bardzo dotkliwe".

Zdaniem Johnsona „każdy zasób, o którym nic nie wiemy może być „potencjalną bombą zegarową". Zawiadomienie o naruszeniu nie podlega przedawnieniu. Utylizacja zasobów IT nie jest czymś, co można ignorować. Powiedziałbym nawet, że jeśli zostanie to zignorowane, stanie się problemem".

Wiele firm może nadmiernie koncentrować się na metodach niszczenia, takich jak czyszczenie za pomocą oprogramowania, zarówno w siedzibie firmy, jak i poza nią; niszczenie niektórych rodzajów nośników; lub rozmagnesowanie. Niektóre organizacje tworzą również szczegółowe zasady dotyczące wielkości niszczenia i zakładają, że jeśli chodzi o możliwość zapobiegania odzyskiwaniu danych z nośnika, im mniejszy, tym lepiej.

„To naprawdę mija się z celem" – powiedział Hoffman. Zamiast tego osoby zarządzające muszą mieć możliwość monitorowania stanu swoich zasobów zawierających dane przez cały cykl ich życia. „Czyli od zakupu, przez cały okres eksploatacji, aż do ostatecznej utylizacji".

Właśnie takie całościowe podejście, od początku do końca, jest ważne przy tworzeniu programu utylizacji zasobów IT - stwierdzili zarówno Hoffman, jak i Johnson.

Jakie jest rozwiązanie?

Wyższa kadra kierownicza może nie być bezpośrednio zaangażowana w decyzje dotyczące utylizacji zasobów IT, ale mimo to jest wiele rzeczy, które te osoby mogą zrobić, aby zrozumieć i zmniejszyć związane z tym ryzyko. Pomoże to w stworzeniu kompleksowego podejścia i solidnego programu utylizacji urządzeń elektronicznych. Właściwy proces powinien być postrzegany jako inwestycja w bezpieczeństwo danych i zrównoważony rozwój.

1 Zidentyfikuj wrażliwe dane

Skoncentruj się na systemach i postaraj się zrozumieć, które zasoby firmy zawierają wrażliwe dane i gdzie się one znajdują. Uważa się, że urządzenia przechowujące dane to laptopy, komputery i serwery, ale istnieją również inne sprzęty.

„Dane są obecne w wielu innych urządzeniach, o których zazwyczaj nie myślimy", stwierdził Hoffman, wskazując m.in. na urządzenia do badań medycznych, a nawet kserokopiarki. „Trzeba mieć naprawdę dobre systemy, aby zrozumieć, gdzie znajdują się urządzenia i jakie poufne dane się na nich znajdują".

2 Opracuj spójne zasady i procedury

Osoby zarządzające firmą jak i działem IT powinny pracować nad wdrożeniem spójnych zasad i procedur obowiązujących w całej organizacji. Mogą również zobowiązać się do nadzorowania zgodności (compliance). Można mieć cały segregator zasad i procedur, ale wszyscy muszą ich przestrzegać i być ich świadomi — zwłaszcza w większych, bardziej rozproszonych organizacjach. Szkolenie personelu jest kluczowe.

„Ważne jest, aby wszyscy w Twojej organizacji rozumieli, jakie są Twoje zasady i procedury", powiedział Hoffman. Należy wprowadzić konsekwencje za nieprzestrzeganie tych zasad oraz sposób monitorowania pozwalający upewnić się, że pracownicy rzeczywiście postępują zgodnie z zasadami. „Jeśli nie ma konsekwencji, ludzie na ogół nie będą postępować zgodnie z procedurami, a ty będziesz mieć bardzo zdecentralizowany i wymagający ciągłego łatania system".

3 Skoncentruj się na bezpiecznym łańcuchu kontroli (chain of custody)

Skoncentruj się na bezpiecznym łańcuchu kontroli (chain of custody) i charakterze danych, a nie na uniwersalnym podejściu do procesów i metod zrządzania danymi.

Chodzi o to, aby osoby decyzyjne oceniły, czy dane są wrażliwe, czy nie. Niejawne dane mogą zostać zniszczone na miejscu. Zwyczajne, mniej wrażliwe dane, takie jak harmonogramy lub adresy, można usuwać poza siedzibą firmy, o ile istnieje bezpieczne połączenie między siedzibą firmy i ostatecznym miejscem przetwarzania.

4 Bądź sumienny w wyborze dostawcy

Aby wyeliminować słabe ogniwa, osoby zarządzające powinny upewnić się, że ich organizacje starannie wybierają dostawców i szukać strategicznych partnerów, a nie zwykłego usługodawcy. Szukaj kontrahentów, którzy przestrzegają wszystkich przepisów i najlepszych praktyk branżowych. Wybieraj wiarygodnych partnerów w procesie utylizacji zasobów.

Ważnym, pierwszym krokiem jest wybór partnerów zewnętrznych posiadających certyfikaty dotyczące utylizacji danych, takich jak i-Sigma. Inne przykłady certyfikatów obejmują standardy R2, które mają zastosowanie w utylizacji zasobów IT. Kadra kierownicza powinna zachować należytą staranność przy wyborze dostawcy.

„Nie wystarczy patrzeć tylko na certyfikat" – powiedział Hoffman. „Od czasu do czasu czytamy historie o podejrzanych firmach, które wysyłały elektrośmieci za granicę lub składowały je na wysypiskach. To może skutkować naruszeniem danych i stanowić zagrożenie dla środowiska. Ponownie podkreślam: należy wybierać bardzo wiarygodnych partnerów, gdy pozbywamy się takich zasobów. Trzeba samodzielnie sprawdzić, czy wszystko jest takie, jak powinno".

Należyta staranność może obejmować wizyty w obiektach potencjalnych partnerów, przeglądanie ich zasad i procedur oraz sprawdzanie referencji klientów.

Podstawy

Ogólnie rzecz biorąc, kadra kierownicza odgrywa kluczową rolę w kształtowaniu kompleksowej i bezpiecznej strategii utylizacji zasobów IT w swojej organizacji. Dzięki inwestowaniu w dobrze przemyślany i zaprojektowany plan, osoby zarządzające mogą pomóc w zapewnieniu bezpieczeństwa swoim firmom i chronić je przed kosztownymi naruszeniami danych, grzywnami i potencjalnym uszczerbkiem na reputacji.

„Zrozumienie natury danych, ich wrażliwości, miejsca przechowywania oraz konsekwentne przestrzeganie zasad i procedur to prawdziwy klucz do udanej strategii" – powiedział Hoffman.

Jak dodał Johnson, w dzisiejszym świecie, jeśli nie zajmiemy się bezpieczną utylizacją zasobów IT, ostatecznie stworzy to problem. „To tylko kwestia czasu".

IRON MOUNTAIN®

0801 800 802 | IRONMOUNTAIN.PL

O IRON MOUNTAIN

Firma Iron Mountain Incorporated (NYSE: IRM), założona w 1951 roku, jest światowym liderem w zakresie przechowywania informacji i zarządzania nimi. Firma Iron Mountain, której zaufało ponad 220 000 organizacji na całym świecie i posiada nieruchomości o powierzchni prawie 8 milionów metrów kwadratowych, w ponad 1400 obiektach, w ponad 50 krajach, przechowuje i chroni kluczowe dane i zasoby , w tym najważniejsze informacje biznesowe, wrażliwe dane oraz artefakty kulturowe i historyczne. Dzięki rozwiązaniom obejmującym bezpieczne przechowywanie, zarządzanie informacjami, transformację cyfrową, bezpieczne niszczenie, a także centra danych, przechowywanie dzieł sztuki i logistykę oraz usługi w chmurze, Iron Mountain pomaga organizacjom obniżyć koszty i ryzyko, zachować zgodność z przepisami, odzyskać dane po awarii i umożliwić bardziej cyfrowy sposób pracy.