Nie kradnij komputerów

„Teraz słuchajcie wszyscy” – kontynuował Elwood, prawdopodobnie głośniej, niż to konieczne. „Wprowadź dyscyplinę. To jest tutaj najważniejsze. Nigdy nie kładziesz palca wskazującego na spuście, chyba że masz zamiar strzelić. Wendell zauważył, że kilka głów kiwnęło głowami. Gopal uśmiechał się. Mike spojrzał nieco niecierpliwy. Wendell mógł sobie wyobrazić dyskomfort menadżera, gdy pozwolił Elwoodowi kierować tym przedsiębiorstwem. Prawdopodobnie myślał, że to o jeden ból głowy mniej, a może nawet coś, co spodoba się wszystkim – cóż, w każdym razie połowie zespołu, który się pojawił – ale teraz najwyraźniej zaczął się zastanawiać. To było z pewnością dziwne działanie zespołowe. Nagrywanie starych dysków twardych. Elwood z pewnością był dumnym Teksańczykiem. W drodze na dzikie tereny Elwood dzielił się fragmentami i fragmentami swojego życia, trzymając jedną rękę na kierownicy swojej ciężarówki, a drugą poruszając się powoli po kabinie, gdy mówił. Całkiem zabawne, pomyślał Wendell. Było coś, co od razu budziło sympatię w Elwoodzie i prawdopodobnie dlatego Mike zgodził się pozwolić mu poprowadzić to nieco niekonwencjonalne zajęcie związane z budowaniem zespołu. „Trzymaj broń skierowaną w stronę celu. Nigdy nie odwracaj się z naładowaną bronią. Rozumiem? Zadbajmy teraz o to, abyśmy wszyscy zrobili to miło i bezpiecznie, rozumiesz? Elwood skierował się w stronę tyłu swojej ciężarówki, gdzie miał wystawiony imponujący stojak z bronią. „Więc co chcecie nakręcić? A ty, Wendell? Jesteś nowy, ty pierwszy musisz dokonać wyboru. Wendell poczuł, jak przechodzi go iskra podniecenia. Nigdy tak bardzo nie interesował się bronią i nigdy nie strzelał z niczego większego niż wiatrówka. Ale teraz mógł wybrać, co mu się podobało. – Och, nie wiem. Co byś polecił?" Elwood chrząknął. „Masz mocne ramiona, poradzisz sobie z kopnięciem. Powiedzmy, że wolisz tę niezłą piątkę. Muszę trzymać uchwyt obiema rękami, OK. Z tego, co Wendell zapamiętał z filmów, sądził, że „oh-pięć” służy do strzelania do samolotów, ale najwyraźniej istniał pistolet tego kalibru. Wybrał ciężką, masywną rzecz i zajął swoje miejsce na linii strzeleckiej. Następny był Imam, trzymający w rękach Wendella karabin szturmowy. Podszedł Elwood. „Nie martw się, wielkoludzie. Będzie dobrze." Uśmiechnął. – Jesteś zdenerwowany? „Podekscytowany” – odpowiedział Wendell. "To proste. Widzisz ten stary dysk twardy tam, na linii 25 jardów? Celuj tak, jak ci pokazałem, zrób wydech i strzel. Najpierw przygotuję dla ciebie klip AP, a potem przełączymy cię na punkty holer. Zobaczysz różnicę, kiedy trafisz w cel. Zachichotał. „Jeśli trafisz w cel”. „Zrobię, co w mojej mocy” – powiedział Wendell i niezależnie od tego, jak bardzo Elwood próbował go przestraszyć, i tak był zdumiony odrzutem, gdy strzelił. Te dwie godziny minęły w chmurze głośnych huków, dymu i śmiechu, podczas gdy powoli odprężali się i zaczęli dobrze bawić. Trzeba przyznać, że Elwood dopilnował, aby nigdy nie popadli w lekkomyślność, więc nikt nie próbował żadnych sztuczek Johna Wayne'a. „Czas położyć krzesła na wozie” – powiedział Elwood. „Więc kto wygrał?” zapytał Imam. Później, z pudłem pełnym starych dysków twardych, z których większość miała duże dziury, grupa wracała do biura. „Słyszałem, że chcesz cholerny domowy system multimedialny?” Elwood zapytał Wendella, żując gumę. Wendell zauważył, że ma tłuste plamy na koszuli. Z drugiej strony Elwood był nieskazitelny. "Tak. Pewnie słyszeliście, że rozmawiałem o tym z Danielem i Cezarem. Więc. Jak to działa, że można zabrać system z biura do domu?” Elwood cmoknął. „To całkiem proste. Po prostu wypełnij formularz systemu domowego, a następnie uzyskaj zgodę Mike'a. Przynieś mi formularz, a wtedy skonfiguruję ci stary system. „Stary system?” Wendell zmarszczył nos. „Te systemy, które właśnie wymieniono, są dość zepsute. Czy jest jakiś sposób na zdobycie czegoś trochę nowszego?” „No cóż, trzymaj się, partnerze. Jesteś tu dopiero od kilku miesięcy. Elwood uśmiechnął się. „Nie oczekuj, że dam ci nagrodę w postaci jałówki!” „No cóż, przynajmniej musi istnieć sposób na dodanie kilku starych dysków”. „Jasne, mam ich całe pudło z dziurami na tyle ciężarówki!” Elwood zachichotał, a potem skinął głową. „Właściwie mam w biurze inne pudełka, które są nadal naprawdę dobre, szkoda byłoby w nich wszystkich dziurawić. Jasne! Myślę, że mógłbym dodać kilka do twojego systemu, ale nadal musisz skrupulatnie śledzić wszystkie zasoby, nawet te, które dzisiaj kręciliśmy. Jeśli dysk ma jakikolwiek adres IP, nie opuści

budynku, chyba że wyrzucę go do niszczarki. Nie chcesz, żeby te dyski pokazywały się w serwisie eBay czy coś takiego. Wendell przeczytał wystarczająco dużo historii o ludziach, którzy wpadali w kłopoty, myśląc, że mogą zarobić dodatkowe pieniądze, sprzedając złom firmowy w Internecie. "Oczywiście nie." „Kiedy wrócimy, pokażę ci stosy palet dyskowych czekających na zniszczenie”. Elwood włączył radio. Dźwięk muzyki country wypełnił kabinę. „Nie mów szefowi, ale zaledwie kilka dni temu zabrałem do domu prawie nową macierz dyskową”. Elwood pochylił się, jakby miał wyjawić tajemnicę, ale nie mógł powstrzymać podekscytowania i powiedział jeszcze głośniej: „Powiem ci, czekałem, aż będzie dostępny, odkąd w zeszłym kwartale pojawił się sprzęt zastępczy. Był używany na produkcyjnym serwerze bazy danych dla zespołu BI, ale dział go wymienił, ponieważ nie miał odpowiedniej pojemności. Poszli do Belindy i sprofilowali ich pamięć masową, ale nie mogła przydzielić im żadnych dysków o wysokiej wydajności z innych projektów, więc kupili nowy. Ten, którego się pozbyli, oznaczyłem w systemie inwentarza jako nadwyżkę sprzętu. Wendell pokiwał głową, wciągnięty. „Więc podłączyłem go do prądu w zeszłym tygodniu, żeby zaaklimatyzował się do temperatury i wilgotności w moim pomieszczeniu multimedialnym, a potem uczynię z niego mój domowy rejestrator DVR i moją bibliotekę filmów. Pokażę ci, kiedy wrócimy, i może zechcesz mi pomóc w konfiguracji. „Pewnie. Jak duża jest tablica?” – zapytał Wendell. „To zewnętrzna macierz z 16 dyskami.” „Będziesz w stanie zapisać na tym sporo programów” – zażartował Wendell. „Tak, do cholery.” „Co używasz jako serwer multimediów?” Elwood spojrzał w tamtą stronę i mrugnął. „Mam serwer, który został zakupiony jako zapasowy kilka lat temu. Nikt nigdy nie korzysta z serwerów zapasowych, więc zabrałem je do domu jako system domowy”. Mówiąc teraz głośniej: „I z pewnością potrzebuję teraz więcej przestrzeni. Gopal i ja znaleźliśmy całą masę filmów w plikach działu marketingu. Chcę mieć ich kopie w mojej bibliotece filmów, zanim Belinda przyjdzie zadawać pytania lub je usunie. Zachichotał. Wendell zacisnął usta. „Słyszałem, że w marketingu jest facet, który wydobywa Bitcoin”. „Cholera. Naprawdę?" Elwood potrząsnął głową. „Z pewnością to dzika banda”. – Więc dobrze się dzisiaj bawiłeś? Wendell uśmiechnął się. „Tak, to była świetna zabawa. Powinniśmy sprawić, że będzie to nasze regularne zajęcia integracyjne.” Elwood uderzył go lekko w ramię. „No cóż, w przyszłym miesiącu to drugie pudełko trafi na złom, więc będziesz mógł spróbować jeszcze raz. Co mówisz?" Wendell potarł ramię. "Brzmi wspaniale." Elwood zachichotał i zwiększył głośność radia.

W Twojej dłoni

Zajęliśmy się trudną koncepcją przypisywania wartości oprogramowaniu. Dopiero w niedawnej historii ludzkości osiągnęliśmy zdolność (i potrzebę) tworzenia produktów, które nie mają fizycznego rozmiaru ani wagi, a większość z nas wciąż instynktownie zmaga się z powiązaniem tego samego poziomu własności z własnością cyfrową, co w przypadku dóbr materialnych , co powinno znacznie ułatwić temat tego rozdziału. Nie kradnij komputerów – to powinno być oczywiste. Niestety rzeczywistość pokazuje inny obraz. Ludzie znacznie lepiej rozumieją własność fizyczną, ale zdolność ta jest sprzeczna z innymi pierwotnymi instynktami, które przywieźliśmy ze sobą z prehistorycznych sawann do centrum danych – potrzebą gromadzenia zasobów w obliczu niedoboru. Rewolucja cyfrowa nie różni się od ogromnych zmian społeczno-gospodarczych, które miały miejsce pod koniec XVIII i na początku XIX wieku, kiedy maszyny przejęły pracę fizyczną i stworzyły potężny efekt fali migracji, zmian i możliwości. W stosunkowo krótkim czasie w miarę stabilny rynek przekształcił się w coś, co wydawałoby się zupełnie obce ludziom zaledwie z poprzedniego pokolenia. Pod koniec XX wieku nastąpiła podobna zmiana w podziale pracy na całym świecie. Komputer uczynił świat mniejszym i szybszym, połączył miliardy ludzi podczas wirtualnego wieczoru i stworzył ogromne możliwości innowacji i wzrostu. W niespotykanym dotąd tempie inżynierowie elektrycy, fizycy i dziwni buntownicy studiujący tajemną sztukę informatyki nagle stali się pionierami zmian. A wśród nich administratorzy systemów stali się strażnikami nieskończonego bogactwa danych i zasobów fizycznych. Niewiele osób pracujących w branży IT uważałoby się za kwatermistrzów gigantycznych magazynów, pełnych wirujących,

hałaśliwych maszyn, regałów z drogim sprzętem, uroczo eleganckich laptopów, ton zapomnianych kabli, myszy i monitorów, a wszystko to pod kontrolą. Niezależnie od tego, czy opiekują się dyskami półprzewodnikowymi, czy belami jedwabiu, instynkty są takie same. Kradzież jest rażąco oczywista i dlatego niewiele osób zdecydowałoby się na kradzież zasobów sprzętowych swojej firmy. Wymyśliliśmy jednak wiele innowacyjnych sposobów na łagodniejsze postrzeganie rzeczywistości, które pozwalają nam uciec od tego, czego w zasadzie nikt by nie pomyślał. Wśród wielu profesjonalistów w świecie IT technicy centrów danych, administratorzy systemów i personel pomocniczy to ci, którzy mają największy dostęp – a tym samym największą pokusę – do zasobów sprzętowych. Każdego dnia niezliczone zasoby są dodawane, usuwane lub spisywane z list inwentarza. Niezależnie od tego, jak zorganizowane są te bazy danych, zawsze istnieje pewien odsetek zagubionych elementów. Niemal zbyt łatwo jest zdecydować, że ten „zagubiony" sprzęt tak naprawdę nie należy do nikogo. Firmy mają również agresywną politykę zarządzania sprzętem, która często koncentruje się na umowach wsparcia, a nie na samej rzeczy stan użyteczności zasobów sprzętowych. Nie ma na Ziemi administratora systemu, który nie ubolewałby nad marnotrawnym (przedwczesnym) likwidacją serwerów lub laptopów tylko z powodu arbitralnych dat w planowaniu zasobów przedsiębiorstwa (ERP). Instynktownie czujemy potrzebę „ratowania" tego sprzętu, ponieważ tysiące lat temu nasi przodkowie tak naprawdę nie mieli żadnych części zamiennych. Łatwym sposobem usprawiedliwienia dziwnego aktu dobroci Robin Hooda jest ponowne wykorzystanie zasobów wycofanych z eksploatacji (EOL) w sposób, który nadal zapewnia luźne powiązanie zasobów z firmowymi bazami danych. Niektóre firmy zachęcają swoich pracowników do ponownego wykorzystania starszych systemów, ale dość często istnieje podziemna praktyka wykorzystywania zasobów niezgodnie z ich przeznaczeniem. Uzasadniamy takie decyzje życzliwością działań oraz faktem, że działania te mają charakter tymczasowy, tzn. pracownicy „pożyczają" stary sprzęt, a nie „biorą go na stałe". Bezpieczeństwo tkwi także w liczbach. „Wszyscy to robią" było popularną wymówką od zarania dziejów ludzkości. Wreszcie, z biegiem czasu ludzie stają się znieczuleni na drobne akty niewłaściwego postępowania. Nie jest to zjawisko charakterystyczne tylko dla branży IT, ale jest dość powszechne w każdej organizacji, w której występuje duża liczba ruchów i zmian zasobów. Na przykład niekoniecznie uważałbyś się za przestępcę zabierając do domu tanią myszkę lub stary, zakurzony kabel sieciowy. Najprawdopodobniej nikt nie zauważy ani nie będzie miał nic przeciwko Twojemu przywłaszczeniu z tych samych powodów, a Ty możesz skojarzyć brak karnej kontroli jako uzasadnienie swojego działania. Z kolei, czując się bezpieczny i prawy, możesz zrobić to ponownie, kierując się instynktem gromadzenia, który jest starszy od produktów na bazie krzemu o dobre kilka tysiącleci. Z biegiem czasu możesz całkowicie stracić taką ocenę. Dopóki ktoś nie zauważy i wtedy stracisz pracę przez pozornie błahą sprawę. Kradzieże pracowników to kosztowna sprawa – w samych Stanach Zjednoczonych kradnie się rocznie około 50 miliardów dolarów1. Tak duże liczby pokazują, że duża liczba osób pada ofiarą drobnych przestępstw, a także niezdolność przedsiębiorstw do dokładnego monitorowania i rozliczania cały ich majątek. Przy tak wielu elegancko zaprojektowanych komputerach i pozornie nieskończonej liczbie urządzeń, kontrolowanie krajobrazu sprzętowego wydaje się trudne i złożone. Rzeczywiście, specjaliści IT znajdują się w niepewnej sytuacji. Oczekuje się od nich, że opracują innowacyjne rozwiązania, które pomogą zapewnić bezpieczeństwo środowiska pracy – mogą nawet zostać pociągnięci do odpowiedzialności, gdy coś pójdzie nie tak. Jako strażnicy mają także najłatwiejszy dostęp do ogromnych łupów i bogactw, jakie stanowi ich środowisko IT.

Nie kradnij (komputerów)

Na papierze kradzież jest prosta do zdefiniowania – jest to przejęcie mienia bez zgody właściciela. Powinieneś mieć w tej kwestii jasne stanowisko – jeśli nie kupiłeś go sam (co będzie miało miejsce w większości scenariuszy pracy), nie należy on do Ciebie. W rzeczywistości jednak kradzież jest trudniejsza do zdefiniowania, ponieważ ludzie naginają zasady i definicje tego, co stanowi własność,

własność i zgodę. Jako ludzie mamy tendencję do wypełniania luk, gdy je znajdziemy, w procesie, zachowaniu i zasadach; i często robimy to na naszą szkodę. W tym celu powinieneś pamiętać podstawowe założenie tego przykazania i zawsze używać go jako punktu wyjścia do wszelkich rozważań związanych ze sprzętem.

Jeśli potrzebujesz sprzętu, kup go

Poruszanie się po systemach zarządzania aktywami może być dość trudne i czasochłonne. Dość często administratorzy i inżynierowie systemów nie mają dostępu ani pozwolenia na dostęp do większości firmowych baz danych. Dlatego pracownicy nie powinni samodzielnie próbować łamać skomplikowanych równań dotyczących zapasów. Zamiast tego powinni trzymać się prostej formuły: jeśli potrzebują danego aktywa, powinni go kupić. Niezależnie od tego, czy jest to superdrogi serwer, czy tania płyta rozwojowa, zawsze należy podchodzić do sytuacji w sposób spójny i przejrzysty. O potrzebne zasoby należy zwrócić się do swojego przełożonego lub odpowiedniego organu. Mogą następnie przekazywać takie żądania dalej w łańcuchu, aż zostaną spełnione. O ile czekanie, aż administracyjny gigant napnie ramiona, może być dość frustrujące (pomyśl o Vogonsie z „Autostopem przez Galaktykę"), o wiele bardziej frustrujące jest, gdy Twoja historia zatrudnienia zostanie skażona czymś tak trywialnym jak kawałek sprzętu.

Kupuj to, czego potrzebujesz, kiedy tego potrzebujesz

„Był używany na produkcyjnym serwerze bazy danych dla zespołu BI, ale wydział wymienił go, ponieważ nie miał do tego prawa pojemności. Poszli do Belindy…"

Ten przykład pokazuje dobrą praktykę zarządzania sprzętem. Kiedy grupa BI zdała sobie sprawę, że ich istniejący serwer może nie nadawać się już do tego celu, nie spieszyła się po prostu z modernizacją urządzenia. Najpierw przeprowadzili dochodzenie, aby dowiedzieć się, czy wystąpił problem z wydajnością czy wydajnością. Umożliwiło im to znalezienie optymalnego obejścia problemu. Być może od początku mogli dokonać lepszego wyboru przy wyborze sprzętu, ale mimo to zastosowali właściwą metodologię przy rozwiązywaniu problemu. Rozwiązania brute-force dla różnych wąskich gardeł baz danych nie są rzadkością. Ze względu na ograniczenia czasowe, wiedzę lub priorytety zespoły IT często wybierają najprostszą odpowiedź – modernizację sprzętu – nawet bez pełnego obrazu problemu i jego symptomów. Dość często takie incydenty będą się powtarzać, szczególnie jeśli są spowodowane błędami logicznymi w oprogramowaniu lub obciążeniu pracą.

Nieużywany sprzęt nie jest Twój

„Nie mów szefowi, ale zaledwie kilka dni temu zabrałem do domu prawie nową macierz dyskową".

Naruszenie przykazania przez Elwooda jest dość rażące. Działał bez zezwolenia i używał sprzętu w niezamierzonym celu. Co więcej, nowa macierz dyskowa nadal ma wartość księgową. To działanie ma wiele konsekwencji. Zabranie do domu sprzętu, który został niedawno zakupiony, nie może być nawet błędnie zinterpretowane jako zwyczajnie tolerowana zła praktyka.

„Oznaczyłem to jako nadwyżkę sprzętu w systemie inwentaryzacji".

Elwood jeszcze bardziej pogorszył problem, błędnie oznakowując sprzęt. Firmy często mają rygorystyczne zasady zarządzania sprzętem, a czasami rządy i gminy przyznają ulgi podatkowe na określone rodzaje działalności biznesowej. Możliwe, że Elwood wplątał swoją firmę w oszustwo podatkowe, błędnie klasyfikując aktywa. Dodatkowo na listach inwentarzowych znajdują się obecnie pozycje błędnie obrazujące stan środowiska IT. Może to na przykład prowadzić do niedokładnych prognoz zakupów opartych na nieprawidłowych danych lub dział biznesowy, który spodziewa się

znaleźć wystarczające zapasy określonego rodzaju sprzętu, może nagle zorientować się, że jest on niedostępny.

„Więc podłączyłem to w zeszłym tygodniu."

Jednak największym problemem w działaniu Elwooda jest to, że zabrał dyski, które były wcześniej używane w produkcyjnej bazie danych. Jest całkiem możliwe, że dyski te zawierają poufne dane. Nie podjęto żadnych działań w celu identyfikacji i usunięcia danych w zatwierdzony i bezpieczny sposób. Podłączając dyski do swojego systemu multimedialnego, Elwood mógł nawet ujawnić dane w Internecie.

„Nikt nigdy nie korzysta z serwerów zapasowych, więc zabrałem je do domu jako mój system domowy."

Wiąże się to z niewłaściwym zarządzaniem zapasami. Może się zdarzyć, że inny zespół w firmie będzie potrzebował serwera do swojej pracy i odkryje, że go brakuje, dopiero wtedy, gdy będzie mu rzeczywiście potrzebny. Nawet jeśli Mike zgodził się na użycie dysku zapasowego, serwer musi zostać odpowiednio sklasyfikowany. Na przykład, jeśli serwer zostanie zabrany do domu i używany do celów dyżurowych lub szkoleniowych, powinien pozostać w księgach. Jeżeli jednak serwer oddawany jest pracownikowi na użytek własny, wówczas należy go wykreślić z ksiąg. W niektórych jurysdykcjach może to również oznaczać przeniesienie wartości serwera na pracownika jako dochód z podatków. W takim przypadku powinna istnieć prawidłowa procedura wyłączania serwera przed ponownym jego przeznaczeniem do innych celów.

„Słyszałem, że w marketingu jest facet, który wydobywa Bitcoin".

To kolejny przykład kradzieży – wykorzystywania majątku firmy do celów osobistych jeszcze w budynku. Nie ma znaczenia, czy sprzęt służy do przechowywania plików multimedialnych, czy do generowania przychodów poprzez obliczenia, w obu przypadkach zmniejsza dostępną pojemność IT, w wyniku czego moc, pamięć masowa i cykle procesora są wykorzystywane do potrzeb osobistych, a nie do zamierzonych celów biznesowych. W ostatecznym rozrachunku przekłada się to na niesankcjonowane działania, które mogą wyrządzić firmie wiele szkód, w tym zarówno reputację, jak i wysokie kary. Wendell powinien był zgłosić problem z wydobyciem Bitcoinów, aby można go było odpowiednio zbadać i zweryfikować. Stracił także okazję do wprowadzenia zabezpieczeń, które mogłyby pomóc w wczesnym wykryciu podobnych nadużyć.

Historia z okopów IT: Pracując jako administrator systemu UNIX w firmie z branży lotniczej, otrzymałem w porze lunchu skargi od kilku inżynierów dotyczące spowolnienia sieci. Pomyślałem, że to dziwne, że nikt inny nie narzeka, ale domyśliłem się, że wszyscy byli na lunchu. Podczas następnej przerwy na lunch potwierdziłem, że sieć jest mocno obciążona i spada liczba pakietów. Zauważyłem również, że wielu inżynierów nie było w stołówce i faktycznie siedziało przy komputerach. Najwyraźniej jeden z administratorów systemu UNIX zainstalował w sieci serwerów oprogramowanie do symulacji lotu i teraz inżynierowie „latali razem" codziennie podczas lunchu.

Jeśli potrzebujesz sprzętu należącego do kogoś innego, poproś o pozwolenie

W idealnym świecie można by składać zamówienia na sprzęt i spełniać je szybko i sprawnie. W większości przypadków będą ograniczenia czasowe i budżetowe i będziesz zmuszony improwizować. Jednakże działanie w szarej strefie pomiędzy zakupem sprzętu a niedokładnymi listami zapasów nie oznacza, że powinieneś popełnić błąd po stronie kradzieży. Jeśli potrzebujesz sprzętu, a w środowisku IT są dostępne zasoby, powinieneś zidentyfikować jego właściciela i poprosić o pozwolenie na jego użytkowanie. Takie podejście wyeliminuje sytuacje, w których Twoje działania mogłyby zostać odebrane jako drobna kradzież lub nadużycie stanowiska pracownika IT. Bez względu na to, jak pilne i

pilne są sprawy, nie powinieneś iść na skróty, aby przezwyciężyć niedociągnięcia w polityce pracy swojej firmy.

Nieużywany sprzęt jest tańszy niż ujawniony adres IP

„Jeśli dysk ma jakikolwiek adres IP, nie opuści budynku, chyba że wyrzucę go do niszczarki".

Chociaż niezwykłe zajęcia związane z budowaniem zespołu miały pewne negatywne skutki, Elwood prawidłowo poradził sobie z zarządzaniem starymi dyskami twardymi przed ich wyjęciem. Rozumie potrzebę zabezpieczenia adresu IP i postępował zgodnie z właściwą procedurą, aby pozbyć się wszelkich magazynów, które mogą zawierać poufne dane – szkoda, że nie zastosował tej samej polityki w swoim własnym systemie medialnym! Na koniec możemy jedynie przypuszczać, że Mike (milcząco) zatwierdził to działanie. W tym przypadku Elwood rzeczywiście postępował zgodnie z procedurami.

Jeśli to znajdziesz, oznacza to, że nie jest Twoje

"Jasne! Myślę, że mogę dodać kilka do twojego systemu, ale nadal musisz bardzo skrupulatnie śledzić wszystkie zasoby. Sugestia Elwooda skierowana do Wendella jest niezgodna z polityką. Może być całkowicie możliwe, że Mike zatwierdzi tę prośbę, ale należy to zrobić w jasny i przejrzysty sposób. Wendell powinien wyraźnie zapytać, czy może dodać dyski, nawet jeśli są stare.

Historia z okopów IT: Kiedy byłem menadżerem zespołu administratorów systemu Linux, pozwalałem/upoważniałem pełnoetatowym pracownikom (będącym administratorami systemów) na zabieranie do domu całkowicie zamortyzowanych stacji roboczych w celu wykorzystania ich jako maszyn testowych do celów edukacyjnych. Dowiedział się o tym pracownik kontraktowy tymczasowy i zabrał do domu starą stację roboczą, którą znalazł w laboratorium. Po audycie spisu systemu odkryto, że brakuje stacji roboczej. W wyniku nieuprawnionego usunięcia stanowiska pracy, umowa pracownika nie została przedłużona i oczywiście został poproszony o zwrot stanowiska pracy.

„Gopal i ja znaleźliśmy całą masę filmów w plikach działu marketingu".

Zasadniczo jest to kradzież miejsca na dysku firmy do użytku osobistego. Obejmuje naruszenie czwartego przykazania (Nie kradnij własności intelektualnej), a także temat naszego rozdziału. Być może nie ma fizycznej kradzieży dysków twardych, ale wykorzystanie pamięci zmniejsza dostępną pojemność do pracy w dziale marketingu. Nieświadomy problemu dział może być zmuszony do zakupu dodatkowych dysków, co wiąże się z kosztami i marnotrawstwem.

Historia z okopów IT: Administrator systemu w naszym zespole uruchomił w pomieszczeniu laboratoryjnym stary serwer plików online i podłączył go do sieci zewnętrznej. Zamknął je tak, że tylko on miał do nich dostęp. Następnie zaczął pobierać na dysk pornograficzne pliki JPEG. Odkryliśmy to podczas usuwania starego sprzętu z laboratorium.

Elwood i Gopal również powinni byli zgłosić niewłaściwe użycie. Jest całkiem prawdopodobne, że filmy zostały pobrane nielegalnie i nawet jeśli stanowią legalną własność zaangażowanych osób, przechowywanie ich na dyskach firmowych najprawdopodobniej stanowi naruszenie warunków licencji. Jednak możliwe jest również, że dział marketingu miał te filmy jako inspirację – lub do wykorzystania w materiałach promocyjnych! W takim przypadku mogli naruszyć procedury, nie prosząc o wykorzystanie w tym celu magazynu na miejscu. Może to być również zwykła kwestia niewystarczającej komunikacji lub niekompletnej dokumentacji, którą należy naprawić, aby poprawnie odzwierciedlała prawidłowe wykorzystanie udziału plików.

Wejście na szczyt gry sprzętowej

Zapobieganie kradzieży sprzętu ma dwa główne oblicza – aktywne środki odstraszające przed sprzeniewierzeniem i niewłaściwym użyciem oraz dokładne zarządzanie sprzętem. Łącznie te dwa podejścia mogą zminimalizować szkody spowodowane przez kradziony sprzęt. Jeśli zabezpieczenia nie powstrzymają kradzieży, skuteczne systemy utrzymujące jasny i aktualny obraz zasobów sprzętowych pomogą wcześnie wykryć incydenty. Co więcej, muszą istnieć jasne, proste i łatwo dostępne zasady wyjaśniające wykorzystanie sprzętu na wszystkich etapach cyklu życia aktywów. Dzięki temu pracownicy będą wiedzieć, co mogą zrobić ze sprzętem, a w przypadku pytań lub wątpliwości będą mogli szybko znaleźć odpowiedź. Usunięcie szarych obszarów zmniejszy niejednoznaczność moralną i usunie pokusę nadużyć.

Zbrodnia doskonała

Zanim przejdziemy do szczegółów usuwania sprzętu komputerowego z miejsca pracy, porozmawiajmy najpierw o niewłaściwym używaniu sprzętu komputerowego w pracy. Istnieje jeden rodzaj kradzieży, który może być dość trudny do wykrycia i zapobiegania: jest to kradzież sprzętu bez usuwania go z budynku. Czasami ludzie mogą wykorzystywać (a raczej niewłaściwie) zasoby pracy dla osobistych korzyści. Wykrycie takich przypadków może być dość trudne, na przykład osoba korzystająca z firmowej licencji na oprogramowanie (np. Matlab lub Photoshop) do przechowywania danych osobowych, nawet jeśli warunki użytkowania i umowa o pracę mogą tego zabraniać. Mogą też używać drogiego serwera do kompilowania swojego osobistego kodu. Ze względów praktycznych obraz lub algorytm używany do celów osobistych jest praktycznie nie do odróżnienia od obrazu lub algorytmu używanego w zadaniu służbowym; niestety narzędzia systemowe zazwyczaj nie sygnalizują tego typu naruszeń. Najlepszym sposobem na ograniczenie tej „miękkiej” kradzieży są szkolenia, dokumentacja i pragmatyczne zasady, które starają się zrównoważyć rozsądne praktyki pracy z potrzebami pracowników. Środowisko promujące uczciwość na wszystkich poziomach pomoże również ludziom zachować etykę. Działa to również w drugą stronę: jeśli pracownicy przyjmą podejście etyczne, straty kapitału w wyniku kradzieży będą mniejsze, a wówczas kierownictwo może być bardziej skłonne do zezwolenia w niektórych przypadkach na wykorzystanie go w celach innych niż praca. Dość często samo nieużywanie sprzętu firmowego do celów osobistych w dużym stopniu przyczynia się do ograniczenia tego typu naruszeń.

Życie komputera

Zarządzanie zapasami sprzętu to jedno z najtrudniejszych zadań w branży IT. Powodów jest wiele. Sprzęt jest dostępny w wielu rozmiarach i kształtach. Oprócz specjalnego sprzętu, jedna osoba bez większych przygotowań jest w stanie udźwignąć większość zasobów sprzętowych. Oznacza to, że w ciągu kilku sekund możesz przenieść laptopa, serwer lub router, co w praktyce oznacza jego utratę. Sprzęt śledzący jest również dość trudny. Umieszczenie etykiety na serwerze jest dość łatwe, ale co się stanie, jeśli zajdzie potrzeba rozebrania serwera na części? Większość sprzętu IT składa się z systemów modułowych z dziesiątkami podzespołów, zaprojektowanych tak, aby były wymienne i wymienne. Ponadto sprzęt komputerowy do funkcjonowania potrzebuje dwóch podstawowych zasobów – energii elektrycznej i sieci . Jeśli te dwa elementy zostaną zapewnione, systemy będą mogły działać w dowolnym miejscu. Możesz mieć stację roboczą w dedykowanym laboratorium na dziesiątym piętrze biurowca lub pod biurkiem. Zmiana lokalizacji fizycznej komplikuje sprawę – ale jeśli odłączysz zasób sprzętowy, stanie się on również niewidoczny dla żadnego agenta monitorującego w środowisku. Co więcej, krajobraz sprzętowy tętni życiem i stale się zmienia. W typowym środowisku IT konfiguracja pracy prawdopodobnie pozostanie niezmieniona przez lata, podczas gdy pracownicy będą przez cały czas korzystać z różnych urządzeń. Sprawa stała się jeszcze bardziej skomplikowana wraz z wprowadzeniem w wielu miejscach pracy zasady „Przynieś własne urządzenie” (BYOD), a także laptopów, tabletów i telefonów komórkowych do środowiska pracy. Nie jest niczym niezwykłym, że w

danym momencie jedna osoba ma przy sobie trzy lub cztery komputery, co stwarza subtelny logistyczny koszmar dla działów IT i bezpieczeństwa. Każde z tych urządzeń wymaga aktualizacji i poprawek, dostosowanych narzędzi i zasad bezpieczeństwa oraz specjalnego oprogramowania; i często są produkowane przez różnych dostawców, z różnymi cyklami życia, harmonogramami i priorytetami. Ponieważ nie ma dwóch takich samych konfiguracji IT, najlepszym sposobem obsługi sprzętu jest śledzenie jego podróży od zakupu do ostatecznej likwidacji, podczas której jest on fizycznie usuwany z siedziby firmy i usuwany z ksiąg.

• Zakup – potrzebujesz procesu zakupu nowego sprzętu. O procesie tym najprawdopodobniej będzie decydował dział finansowy, a nie dział IT, ale informatycy pomogą w wyborze i zaprojektowaniu systemu zakupów.

• Nabycie i wyładunek – musi istnieć proces odbioru, katalogowania i wprowadzenia zakupionego sprzętu do środowiska IT.

• Zapasy – wymagana jest także baza zapasów (pisemne zapisy, arkusz kalkulacyjny, narzędzie ERP), która będzie zawierała listę zakupionego sprzętu zgodnie z polityką. Godne uwagi szczegóły w tej bazie danych będą obejmować:

• Każdy zasób powinien mieć jakiś unikalny identyfikator. Identyfikator ten pozwoli każdemu odnaleźć zasób, dlatego powinien być zarówno zarejestrowany w odpowiedniej bazie danych, jak i dostępny do fizycznej kontroli na samym urządzeniu. W niektórych przypadkach urządzenie może być zbyt małe lub niedostępne, aby używać drukowanych etykiet, dlatego można zastosować alternatywne metody cyfrowe.

• Każdy zasób powinien mieć również lokalizację – a najprawdopodobniej będzie się ona zmieniać w trakcie życia urządzenia. Fizyczne śledzenie sprzętu stanowi wyzwanie, ponieważ urządzenia mogą nie zawsze być włączone i w związku z tym niedostępne przez sieć. Aktywne nadajniki radiowe, takie jak znaczniki RFID lub moduły Zigbee, można wykorzystać do tworzenia podglądu wszystkich dostępnych zasobów w czasie rzeczywistym. Alternatywnie lokalizacja może być aktualizowana ręcznie lub ustalana w sposób algorytmiczny na podstawie sposobu użytkowania urządzenia, ale często może to prowadzić do błędów i nieaktualnych informacji.

• Użytkowanie – w normalnym cyklu życia urządzenia powiązane metadane opisujące urządzenie, w tym numery seryjne, system operacyjny, zainstalowane oprogramowanie, lokalizacja w centrum danych, adres IP i inne właściwości, muszą być przechowywane w spis. Monitoring i audyt pozwalają zidentyfikować te zmiany – a może nawet dokonać automatycznych poprawek w odpowiednich bazach danych.

• Koniec życia (EOL) – zasoby sprzętowe należy usunąć ze środowiska w uporządkowany sposób. W rzeczywistości jest to trudniejsze, niż się wydaje, ponieważ w firmie mogą znajdować się osoby, grupy lub podmioty, które oczekują, że komputery będą działać wiecznie, i mogą mieć zakodowane na stałe zasady dotyczące łączności i użytkowania. Zepsują się one, gdy urządzenia zostaną wyłączone. Co gorsza, niektóre z nich mogą być cichymi awariami skryptów i narzędzi działających w tle bez żadnego monitorowania, a problemy ujawnią się dopiero długo po fakcie.

• Urządzenia należy najpierw wyrejestrować z wszelkich usług dostępnych dla klientów. Umożliwi to administratorom systemu śledzenie wszelkich błędnych prób połączeń lub logowań oraz informowanie dowolnej grupy biznesowej o możliwych lukach logicznych w ich oprogramowaniu. To z kolei może sprawić, że całe środowisko będzie zdrowsze i solidniejsze.

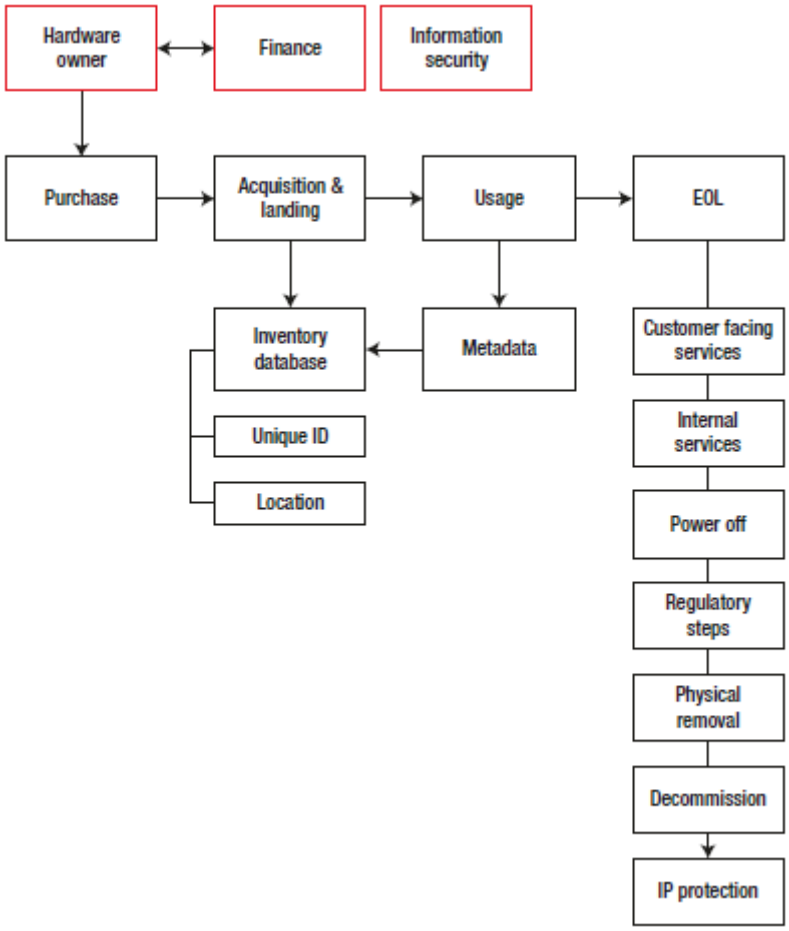
• Następnie należy wyłączyć urządzenia. Czasami nazywa się to również „testem krzyku” – podczas którego oczekujesz, że ktoś zauważy i zacznie narzekać. Równolegle jest to test Twojego oprogramowania monitorującego i alarmującego, które powinno poprawnie odzwierciedlać zmianę stanu urządzenia. Jeśli zasób został odłączony od usług skierowanych do klienta, użytkownicy nie powinni widzieć żadnych widocznych zmian. Odporny system o wysokiej dostępności będzie zachowywać się w ten sposób z założenia, a wymiana poszczególnych komponentów nie spowoduje żadnych zakłóceń ani przestojów.

• Jeśli urządzenia zawierają ważne lub potencjalnie wrażliwe dane, można je pozostawić wyłączone, ale nie usuwane z inwentarza, aby umożliwić jakiekolwiek procesy regulacyjne. Na przykład dział prawny może wymagać archiwizowania nośników z EOL bez żadnych modyfikacji przed usunięciem lub zniszczeniem nośników. Podobnie może zaistnieć potrzeba ponownego dostępu do przechowywanych danych i ponownego włączenia urządzenia w celu pobrania informacji (np. do celów kryminalistycznych).

• Następnie należy fizycznie usunąć urządzenia ze swojej lokalizacji, niezależnie od tego, czy jest to biuro, czy centrum danych, i jednocześnie zaktualizować wszystkie odpowiednie wpisy w bazie danych, aby odzwierciedlić tę zmianę. Powinno to obejmować również wszystkie licencje, oprogramowanie i powiązane informacje. Ważne jest, aby wszystkie te zdarzenia odbywały się synchronicznie, aby uniknąć błędów w inwentaryzacji.

• Na koniec można następnie wycofać urządzenie z eksploatacji w oparciu o klasyfikację urządzenia i zasady firmy. Jak zdefiniowaliśmy we wcześniejszych rozdziałach, chodzi o dane i ochronę własności intelektualnej. Jeśli urządzenie zawiera nośnik dowolnego typu, w pierwszej kolejności należy zająć się aspektami danych. Zwykle dyski twarde wymagają sformatowania lub wyzerowania, a czasem nawet fizycznego zniszczenia. Czasami firmy oddają stary sprzęt organizacjom non-profit i organizacjom charytatywnym i w tym scenariuszu mogą istnieć dodatkowe zabezpieczenia zapobiegające wyciekom danych lub naruszeniom umów handlowych (np. Twój sprzęt trafia do jurysdykcji, która nie jest objęta umowami eksportowymi lub licencje).

Musisz mieć zdefiniowany proces i dokumentację dla każdego etapu „życia” sprzętu. Proste listy kontrolne to najprostszy sposób, aby upewnić się, że technicy i administratorzy systemu wiedzą, co robić w każdej sytuacji. Powinien także istnieć scenariusz „bramy domyślnej”, który uwzględnia każdy przypadek narożny nieobjęty istniejącymi zasadami, a także zawiera listę odpowiednich podmiotów gospodarczych uprawnionych do wykonywania połączeń w takich przypadkach narożnych. Jeśli Twoja firma jest wystarczająco duża, chcesz przypisać właściciela sprzętu, który będzie nadzorował cały cykl życia. Podmiot ten może występować pod różnymi nazwami, np. menedżer centrum danych, menedżer zapasów itp., ale zasadniczo cel będzie ten sam. Osoby na tym stanowisku będą miały możliwość definiowania nowych polityk oraz kierowania ewentualnych pytań do innych funkcji w organizacji, np. zespołu finansowego czy zespołu ds. bezpieczeństwa informacji. Cały cykl przedstawiono na rysunku



Za żelazną kurtyną

Jasne zasady i inteligentne zarządzanie zapasami w dużym stopniu przyczyniają się do stworzenia środowiska IT wolnego od kradzieży. Im więcej zainwestujesz w zapewnienie prawidłowego śledzenia, rejestrowania i aktualizowania sprzętu, tym tańsze będzie to w dłuższej perspektywie. Jednak w niektórych sytuacjach konieczne będzie zastosowanie dodatkowych środków, aby mieć pewność, że sprzęt pozostanie na swoim miejscu. Fizyczne bezpieczeństwo zasobów sprzętowych może budzić podejrzenia u pracowników – podobnie jak w przypadku innych systemów monitorowania skierowanych do wewnątrz. Należy jednak pamiętać, że systemy zabezpieczeń odstraszą zarówno graczy wewnętrznych, jak i zewnętrznych, a granice fizyczne wzmacniają zasady, nawet jeśli w firmie nie dochodzi do niewłaściwego użycia sprzętu. Szpiegostwo przemysłowe jest doskonałym przykładem. Z firm posiadających podmioty na poziomie międzynarodowym podejmowane są próby kradzieży przedsprzedażowych próbek i dysków twardych pełnych wrażliwych danych lub w sposób raczej filmowy włamania się do sieci fizycznej i zainstalowania sprzętu typu Man-in-the-Middle (MITM) która umożliwia nieuczciwej stronie podsłuchiwanie pakietów sieciowych. To nie tylko materiał na książki szpiegowskie i hity kinowe! Następnie mamy do czynienia ze zwykłą, pospolitą kradzieżą. Wyobraź sobie, że ktoś mógłby po prostu wejść do Twojego biura i zabrać ze sobą ładny, błyszczący laptop pozostawiony na biurku podczas lunchu. Omówimy je znacznie bardziej szczegółowo w następnym rozdziale. W tym przypadku celem systemów zabezpieczeń fizycznych jest utrudnienie zgubienia sprzętu i łatwiejsze jego odnalezienie. Sprzęt przeznaczony do stałego lub półtrwałego zamocowania (np. większość zasobów w centrach danych) będzie przechowywany w bezpiecznych obiektach zarówno podczas użytkowania, jak i przechowywania. Udogodnienia będą obejmować różne metody zapewniające, że zasoby sprzętowe (i wszelkie powiązane z nimi adresy IP przechowywane na

nich) nie będą mogły być łatwo dostępne, usuwane ani modyfikowane. Typowe zabezpieczenia obejmują zamki do szaf komputerowych, kamery monitorujące, drzwi z mechanizmami uwierzytelniającymi, szczelne korytarze centrów danych i inne.

• Sprzęt zaprojektowany z myślą o przenośności (np. większość sprzętu biurowego) powinien być zabezpieczony w sposób uniemożliwiający łatwą kradzież. Typowe metody obejmują stacje dokujące z kluczem, blokady kablowe i trzymanie sprzętu w bezpiecznym miejscu, gdy nie jest używany.

• Sprzęt, na którym można uruchomić oprogramowanie, powinien mieć zainstalowany agent monitorujący. Celem takiego modułu jest zapewnienie pulsu sieci – i ewentualnie lokalizacji – do obiektu centralnego. Może to stanowić integralną część szerszego systemu monitorowania. Jeśli urządzenie „odłącza się od sieci", technik IT może wrócić do ostatniej znanej lokalizacji, aby rozpocząć naprawę lub, w przypadku braku sprzętu, przeprowadzić dochodzenie.

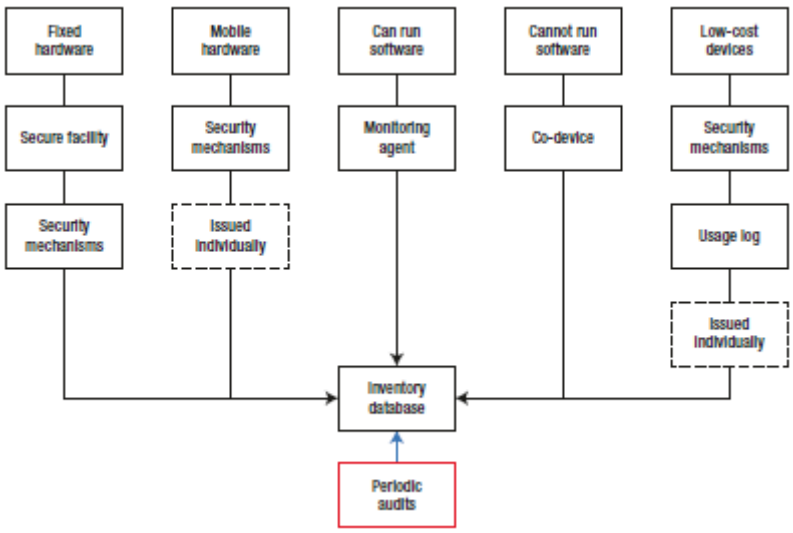
• Jeśli na sprzęcie nie można uruchomić dodatkowego oprogramowania, można użyć fizycznego urządzenia towarzyszącego, aby oznaczyć sprzęt, aby można było go śledzić. Jako (dodatkowy) efekt uboczny upraszcza to również zarządzanie zapasami i może prowadzić ze znacznie większą dokładnością ogólnej (w czasie rzeczywistym) widoczności i stanu środowiska IT.

• Komponenty sprzętowe, które są uważane za zbyt małe lub tanie, aby można je było wyposażyć w znacznik śledzący (takie jak kable zasilające, kable sieciowe lub klawiatury), nadal muszą być odpowiednio skatalogowane i przechowywane. W idealnym przypadku komponenty te będą przechowywane w szafkach lub szafkach, do których dostęp i korzystanie z nich wymaga fizycznej interwencji. Należy odnotować każde użycie (np. przeciągnięcie identyfikatora pracownika w celu uzyskania dostępu do magazynu sprzętu), a wszelkie zmiany w stanie wyposażenia należy odpowiednio zaktualizować w bazie danych sprzętu.

• Urządzenia bez powiązanego śledzenia również muszą zostać sklasyfikowane. Ogólnie rzecz biorąc, istnieją dwie kategorie: sprzęt nieindywidualny, używany głównie do sprzętu zaplecza (serwery, sprzęt sieciowy, telefonia itp.) oraz sprzęt wydawany osobom fizycznym (taki jak klawiatura i mysz). Ten ostatni rodzaj powinien być wydawany pracownikom indywidualnie, czyniąc z każdego pracownika menedżera zapasów własnego sprzętu.

Historia z okopów IT: W jednym z moich poprzednich miejsc pracy wymyślono dość sprytne rozwiązanie problemu ciągłej utraty zestawów słuchawkowych, klawiatur, myszy i innych pozornie niskiej wartości urządzeń. Zainstalowali automaty sprzedające sprzęt, obsługiwane za identyfikator pracownika. Każdy mógł zamówić produkty z dostępnych zapasów, a sprzęt zostałby automatycznie powiązany z jego nazwą. Dzięki temu proces był szybszy i dokładniejszy, mimo że większość pracowników uważała nową metodę za kosztowny chwyt.

Okresowe audyty są kluczowe dla dokładnego zarządzania sprzętem, szczególnie jeśli wszystkie dostępne zasoby są objęte tylko częściowym systemem śledzenia. Audyty pozwalają firmie właściwie i prawidłowo rozliczyć wszelkie rozbieżności lub straty w oczekiwanych ilościach oraz wprowadzić zmiany w konfiguracji operacyjnej, ponieważ obecne metody i narzędzia mogą okazać się niewystarczające. Wykryte luki w możliwości znalezienia całego sprzętu pozwolą właścicielowi centrum danych i administratorom systemu na znalezienie ulepszonych rozwiązań. Ponadto pozwalają także na dokładniejsze prognozy księgowe i zakupowe. Model zabezpieczeń sprzętowych pokazano na rysunku .



Przejrzysty i obecny serwer

Wreszcie, w polityce nie może być dwuznaczności. Nie powinno mieć miejsca sytuacja, w której pracownik mógłby błędnie zinterpretować istniejące ramy procedur i narzędzi, w wyniku czego zacząłby taszczyć do domu zapasowy komputer, nie będąc w pełni świadomym naruszenia. Najprostszym podejściem są rygorystyczne zasady, które zabraniają jakiegokolwiek wykorzystywania majątku służbowego do celów osobistych. Dzięki temu podejmowanie decyzji jest znacznie prostsze. Z biegiem lat wykorzystywanie majątku służbowego do celów osobistych stało się coraz bardziej powszechne i prawdopodobnie będzie rosnąć, w miarę jak zacierają się granice między tym, co kiedyś powszechnie uważano za „biuro" a „dom". Dotyczy to laptopów służbowych, telefonów, a także aparatów fotograficznych, monitorów i podobnego sprzętu, szczególnie w przypadku firm rozproszonych po całym świecie, które zatrudniają pracowników w domu. W takich sytuacjach zarządzanie sprzętem jest trudniejsze, ale nadal powinno być poprawnie i w pełni zdefiniowane. W idealnym przypadku łączyłoby to przejrzystą dokumentację z internetowym portalem samoobsługowym, który umożliwia użytkownikom śledzenie własnego sprzętu, wysyłanie żądań lub sprawdzanie wszelkich odpowiednich procedur.

Wniosek

Administratorzy systemów i technicy centrów danych nie różnią się niczym od dzieci puszczanych w sklepie z zabawkami. Dlatego też są sobie winni pomoc w zbudowaniu jasnych, jednoznacznych i przejrzystych ram zasad użytkowania sprzętu. Na dłuższą metę prowadzi to do solidniejszego, lepiej zorganizowanego i lepiej utrzymanego środowiska sprzętowego, z mniejszą liczbą pokus ulegania prehistorycznej potrzebie gromadzenia danych. Sprzęt musi być odpowiednio klasyfikowany, śledzony i zarządzany. Cykl życia urządzenia musi być mapowany na każdym kroku. Można używać zarówno systemów sprzętowych, jak i programowych, aby stworzyć obraz sytuacyjny środowiska IT, obok dobrze udokumentowanych zasad i procedur oraz okresowych audytów. Wreszcie, zawsze może zaistnieć przypadek narożny, w którym nie ma żadnych zasad ani znanych precedensów. W takich sytuacjach zawsze pamiętaj, aby zapytać, ponieważ kariery są warte więcej niż bryła krzemu i plastiku. Nie kradniemy adresu IP i sprzętu, cóż, można by pomyśleć, że są one czyste. Ale na niezbadanych wodach IT czyhają inne niebezpieczeństwa i pułapki. W następnym rozdziale porozmawiamy o terra incognita, czyli częściach świata IT, do których nie wolno się zbliżać.