Nie idź tam, gdzie cię nie chcą

Wracając z krótkiej przerwy, ostatnią osobą, którą Wendell spodziewał się zobaczyć stojącą za biurkiem, była Frieda z InfoSec. Nigdy nie wyglądała na szczególnie szczęśliwą, ale dzisiaj… wydawała się w złym nastroju. To nie może być dobre, pomyślał, starając się zachować neutralny wyraz twarzy. „Zostawiłeś komputer odblokowany!" – warknęła na powitanie. Wendell skrzywił się. „Masz szczęście, że ktoś nie usunął wszystkich twoich plików!

Może powinienem był zainstalować w twoim systemie wygaszacz ekranu Bielefeld. Co byś chciał? Następnym razem zamknij je, kiedy będziesz wychodzić. Wendell stał jak wryty w miejscu, doskonale świadomy, że głos Friedy się niesie i że wszyscy jego koledzy przestali pracować i przyglądają się całej scenie. Był oszołomiony i trochę przestraszony. Ostatnią rzeczą, jakiej potrzebował, była nagana od Friedy przed trzymiesięczną oceną z Mikiem. Potem rozjaśniło mu się w głowie i zaczął się zastanawiać: co to jest Bielefeld? „I jesteś zalogowany jako root" – kontynuowała Frieda, wykorzystując jego milczenie jako okazję do wtrącenia swojej uwagi. „Na więcej niż jednym terminalu. Mogłem usunąć bazę danych klientów!" „Ech, cóż, właściwie właśnie zalogowałem się na serwer testowy" – wyjąkał Wendell. Frieda zmrużyła oczy. „Nigdy nie wiadomo, do jakiego rodzaju danych ma dostęp serwer testowy. Każdy mógł skopiować pliki klientów." – Hm, wiem, jaki to rodzaj dostępu – zaprotestował Wendell, ale upewnił się, że zrobił to bardzo cicho, w swojej głowie. – Nie było mnie tylko na minutę. „Jesteś złym chłopcem, Wendell" – zażartował Caesar. Frieda zdawała się tego nie zauważać. „Jakie dane masz na temat tego systemu testowego?" Wendell szybko pochylił się i zablokował ekran komputera. "Byłem łazience, a minęło tylko kilka minut. Dlaczego chcesz wiedzieć?" Jego głos wciąż był drżący. „Muszę wiedzieć, na wypadek gdybyś ujawnił poufne dane!" Frieda była na fali. „Czy wiesz, ile kosztuje ochrona badania takiego bałaganu? Będę musiał zdobyć nagrania z monitoringu, sprawdzić dostęp do sieci, sprawdzić użycie USB…" „W moim systemie ani na serwerze testowym nie ma nic poufnego" – wymamrotał Wendell, mając nadzieję, że się wycofa. Zastanawiał się nad tym, co przed chwilą powiedział. To nie było zwykłe kłamstwo, prawda? „Jestem nowym pracownikiem. Nie daliby mi dostępu do tego rodzaju informacji. Frieda prawie podskoczyła. "Nowy pracownik? To dlaczego wczoraj widziałem cię w centrum danych na monitorze bezpieczeństwa? Bez wpisywania się do dziennika dostępu!" Patrzyła prosto na niego i zaczynała pochylać się do przodu. „Jaką działalność prowadzisz w centrum danych?" Wendell wskazał za siebie. „Właśnie odwiedzałem Elwood i oprowadził mnie po okolicy". „Nie ma żadnych wycieczek po centrum danych. To bezpieczny obszar. Myślałeś, że jesteś na zamku Neuschwanstein? Uśmiechnęła się. „Hej, Frieda, daj spokój naszemu „Dellowi" – odezwał się Elwood, podchodząc. Poklepał Wendella po plecach. „Oprowadziłem go po okolicy, żeby wiedział, jak wszystko działa, jeśli coś się zepsuje. Zostawił telefon, a ja byłam przy nim przez cały czas. Frieda nie wyglądała na udobruchaną. „Co robiłeś przy tym serwerze w H12? Wendell myślał, że podał jej powód przebywania w centrum danych. „Sprawdzałem mój serwer testowy. Mam na myśli VM. Nie wiedziałem, na jakim hypervisorze to działa. Jak mnie widziałeś?" „Lepiej uważaj, gdzie idziesz, bo ja jestem". Frieda nie cofała się, wpatrując się w niego i prowokując do mrugnięcia okiem. „Czy widziałeś jakieś poufne dane, gdy byłeś w centrum danych?" „Nic nie widział" – powiedział Elwood. Wendell zauważył, że Elwood wyglądał na rozbawionego. Ale w całej tej sytuacji nie widział nic zabawnego. Potem przypomniał sobie, że jedna z konsol była otwarta i wyświetlała na ekranie jakieś dane. – Och, nie – powiedział szybko. „Właśnie widziałem stojaki z komputerami. Czego ode mnie potrzebujesz?" "Co się dzieje?" Wendell odetchnął z ulgą. To był Mike. Wendell zdał sobie sprawę, że Frieda wydawała się być równie wrogo nastawiona. Nie było to więc nic osobistego przeciwko niemu ani jakiś trik, jaki zrobili nowym pracownikom. „Seria naruszeń bezpieczeństwa informacji, oto co się dzieje…" „Słuchaj" – wtrącił się Mike. „Mówmy o tym cicho, ludzie próbują pracować. Wendell to nowy chłopak, więc musisz dać mu trochę luzu. Być może popełnił jeden lub dwa błędy, ale w ten sposób wszyscy się uczymy. Poprosiłem go, aby dowiedział się jak najwięcej o środowisku i wszyscy byli

pomocni, więc jeśli masz jakieś skargi, możesz je skierować do mnie. Frieda prychnęła. Wyglądała na niezadowoloną – i podejrzliwą. – Może uda ci się porozmawiać z Gopalem. Może udzielić ci dodatkowych wskazówek" – powiedział Mike. Wendell skinął głową. W tym momencie zgodziłby się prawie na wszystko, żeby tylko mieć spokój z InfoSec. – Jasne, Mike. „Nadal cię obserwuję" – powiedziała Frieda, odchodząc. Wendell opadł na krzesło. "Co to było do cholery?" Alex podniósł głowę i uśmiechnął się. „To było, mój drogi, twoje pierwsze spotkanie z Friedą. Nie martw się, ona po prostu chce cię trzymać z dala od kłopotów. Może." Elwood zaśmiał się. – Biorąc wszystko pod uwagę, poradziłeś sobie całkiem nieźle. Wendell skrzywił się. "Zrobiłem?" Cezar też tam był, cały w przebiegłej wesołości i przesadnym wyrazie twarzy. "O tak. Przynajmniej nie płakałeś. Wszyscy zaczęli się śmiać. Wendell pozwolił swoim nerwom uspokoić się, a potem dołączył, czując się głupio – i zmartwiony.

Oto smoki

Środowiska IT, zwłaszcza centra danych i laboratoria, mogą być wspaniałymi miejscami. Nie różnią się one zbytnio od muzeów prezentujących tysiące ciekawych okazów. Jeśli spojrzysz poza suche dane, zobaczysz duże, złożone labirynty niesamowitych technologii i narzędzi, połączonych ze sobą i zamkniętych w skomplikowanym tańcu cyfrowego życia. Często o tym nie myślimy, ale wyobraźmy sobie, ile wysiłku i precyzji wymaga to, aby pociągi kursowały zgodnie z rozkładem, sygnalizacja świetlna zmieniała się na zieloną, aby miasta mogły się poruszać, lub pozwalała przeglądarce na natychmiastowe udzielanie odpowiedzi na wszystkie pytania. Cała ta niesamowita innowacja jest wynikiem niekończącego się pogoni za wiedzą, która definiuje ludzką naturę. Jesteśmy dociekliwi i ciekawi, i dotarliśmy tu, gdzie jesteśmy dzisiaj, ponieważ przez tysiące lat nieustannie przesuwaliśmy granice tego, co można zrobić w każdym aspekcie naszego życia. Dlatego nie powinno być zaskoczeniem, gdy powiesz komuś, że nie może udać się w miejsce, któremu na pierwotnym poziomie stawiałaby opór. Jeśli chodzi o granice, świat IT wydaje się być zbudowany z paradoksów. Z jednej strony firmy zachęcają swoich pracowników do nieszablonowego myślenia, szukania rozwiązań wykraczających poza znane i przyjęte konwencje i ciągłego doskonalenia. Z drugiej strony firmy tworzą pozornie dowolne „ściany", które mają za zadanie ograniczać dostęp i utrudniać pracę twórczą. W początkach tego, co nazywamy nowoczesnym IT, administratorzy systemów nie mieli praktycznie żadnych ograniczeń. Technologia była rozwijana i wykorzystywana w oparciu o zaufanie – niektóre z tych decyzji są nadal widoczne w dzisiejszym działaniu Internetu i praktycznych ograniczeniach oprogramowania wynikających z hojnych, liberalnych projektów w architekturze. Podejście altruistyczne wkrótce okazało się niewystarczające, ponieważ firmy i organizacje starały się chronić swoją własność intelektualną i zapewnić większą kontrolę nad swoim otoczeniem, zarówno wewnętrznie, jak i zewnętrznie. W niektórych przypadkach zabezpieczenia miały sens, np. w przypadku wojska, rządu i opieki zdrowotnej. W innych przyjęto je z mniejszym entuzjazmem i zrozumieniem korzyści płynących z wdrożonych działań. W miarę rozwoju świata IT (i Internetu) wahadło zaczęło odchylać się od strony permisywnej, co doprowadziło do kolejnych ograniczeń, zarówno w zakresie bezpieczeństwa fizycznego, jak i cyfrowego. Chociaż można debatować nad korzyściami i konsekwencjami moralnymi obecnego krajobrazu technologicznego, praktycznie niemożliwe jest oddzielenie i oddzielenie bezpieczeństwa od podstawowej działalności jakiejkolwiek nowoczesnej firmy. Ta rzeczywistość często powoduje zamieszanie i frustrację wśród osób obsługujących szkielet IT. Na poziomie filozoficznym większość administratorów systemów i programistów zgodzi się, że w chaosie musi być jakiś porządek i że niektóre mechanizmy bezpieczeństwa są naprawdę korzystne dla rozsądnego i wydajnego funkcjonowania wielu środowisk IT. Jednak to uczucie rzadko pojawia się, gdy ludziom w codziennej pracy przeszkadza coś, co często można określić jako niepotrzebną biurokrację i paranoję. Kierując się potrzebą ciągłego doskonalenia się i doskonalenia, ludzie szukają – i znajdują – obejść, które pozwolą im działać szybciej i bardziej produktywnie oraz zapewniać wyniki. Idąc na skróty, narażają się na naruszenia zasad etycznych, które mogą kosztować ich utratę pracy. Co gorsza,

większość ścian oddzielających i chroniących środowiska IT ma charakter efemeryczny. Na przykład zapora programowa to jedynie zestaw reguł „jeśli-to" filtrujących ruch sieciowy. Zmiana ich jest prawie zbyt łatwa, szczególnie dla osób z odpowiednimi danymi uwierzytelniającymi i dostępem. Dostęp fizyczny jest łatwiejszy do zrozumienia i zrozumienia – w podobny sposób ludzie czują się bardziej komfortowo kradnąc oprogramowanie i własność intelektualną niż kradnąc komputery. Postrzeganie namacalnej wartości pomaga nam określić granice i szanować je. W przypadku oprogramowania takie ograniczenia są trudne do uchwycenia i łatwe do zignorowania lub obejścia. Tak się składa, że administratorzy systemu często mają uprawnienia do wprowadzania zmian, jeśli mają na to ochotę. I czasami to zrobią. Jeszcze bardziej komplikujemy sprawę, dodając do obrazu wymiar moralny. Kiedy ludzie omawiają szkolenie w zakresie bezpieczeństwa lub proces uzyskiwania dostępu do bazy danych, nie myślą tylko o bezpośrednich krokach niezbędnych do wykonania zadania lub potencjalnych korzyściach płynących z tych środków dla firmy lub jej klientów. Często wplatają w to całą historię wiadomości, historie internetowe, doświadczenia z przeszłości, a także osobiste stanowisko i opinie, często skażone konotacjami moralnymi, a nawet politycznymi. Programy antywirusowe, czytniki identyfikatorów i biuletyny dotyczące bezpieczeństwa to nie tylko środki zaprojektowane, aby zapewnić bezpieczeństwo firmy – są złożoną sagą emocjonalną. Połączenie władzy, łatwego dostępu, osobistej moralności i potrzeby rozwiązywania problemów to zmienna mieszanka, która sprawia, że ludzie przekraczają – fizycznie i cyfrowo – obszary, do których normalnie nie są dopuszczeni. Stwierdzimy, że działamy, nawet nie zdając sobie sprawy, że to robimy. Dopóki nie wydarzy się coś złego.

Nie idź tam, gdzie cię nie chcą

W sytuacji skażonej dwuznacznością (własną) najlepszym sposobem jest przestrzeganie zasad. Idealnie byłoby, gdyby istniały zasady jasno definiujące dostęp, uprawnienia i potrzebę wiedzy w każdym przypadku związanym z biznesem. Jeżeli te zasady nie istnieją, należy zachować szczególną ostrożność.

• Zasady i ograniczenia istnieją nie bez powodu – mogą to być błędne powody, ale istnieje proces, który doprowadził do wdrożenia zasad. Jeśli chcesz naprawić błąd, powinieneś zająć się źródłem problemu. Co więcej, reguły przypominają logikę monitorowania oprogramowania; dodajesz nowe wpisy, ale rzadko, jeśli w ogóle, usuwasz stare. Z biegiem lat powstają starożytne warunki, które nie mają już zastosowania we współczesnych sytuacjach, lub powody ich wdrożenia zostały już dawno zapomniane. Jeśli chcesz w pełni zrozumieć i uzasadnić zasady, musisz wziąć je pod uwagę. Podobnie, jeśli to możliwe, stare zasady powinny zostać poddane audytowi i przeglądowi pod kątem przydatności oraz uporządkowane w celu uproszczenia procedur pracy.

• Zasady i ograniczenia chronią firmę i Ciebie – ogólnie rzecz biorąc, zasady często ograniczają Twój dostęp, fizyczny lub cyfrowy, ale ich celem jest ochrona wszystkich zaangażowanych – firmy i jej aktywów oraz Ciebie. Istnieją sytuacje, które trudno w pełni zdefiniować za pomocą pisanych zasad (w przeciwnym razie zasady musiałyby być długie i skomplikowane, aby ich stosowanie było niepraktyczne). W takich sytuacjach, zwłaszcza gdy istnieje duże ryzyko szkód – a nawet zagrożenia życia – proste zasady pozwalają na znacznie łatwiejsze i szybsze podejmowanie decyzji.

• Ograniczenia minimalizują ryzyko – niektóre zasady opierają się na koncepcji konieczności posiadania wiedzy. Na przykład dostęp do akt HR musi być ograniczony z oczywistych względów prawnych. Taka decyzja nie ma nic wspólnego z konkretnymi ludźmi, a osobista wiarygodność poszczególnych pracowników nie ma znaczenia przy przyznawaniu dostępu. Podobnie może istnieć wiele innych systemowych baz danych, folderów, udziałów, laboratoriów, obszarów centrów danych, a nawet biur, do których administratorzy systemu nie powinni mieć dostępu. Ważne jest, aby nie wiązać tych

ograniczeń z żadnymi konotacjami moralnymi. Podział na segmenty pomaga firmom bezpieczniej zarządzać danymi i ograniczać szkody kaskadowe w przypadku naruszeń, awarii lub innych komplikacji.

• Nadal obowiązuje zdrowy rozsądek – nie oznacza to, że powinieneś całkowicie ignorować swój wewnętrzny kompas moralny, lekceważyć zdrowy rozsądek i logikę i po prostu ślepo stosować się do instrukcji, bez względu na konsekwencje. Jeśli uważasz, że Twoje działania mogą wyrządzić dalsze szkody lub skomplikować sprawę – nawet jeśli suche zasady mogą całkowicie zwolnić Cię z odpowiedzialności – powinieneś przestać myśleć i ponownie ocenić swoją pracę.

Jeśli znajdziesz uzasadnione powody, dla których istniejące zasady nie są odpowiednie, powinieneś nakłonić odpowiednich właścicieli do wprowadzenia niezbędnych zmian. Ale nie powinieneś ignorować zasad ani obchodzić się z nimi tylko dlatego, że od razu zdecydowałeś, że są bezużyteczne lub głupie. Pytanie dlaczego jest kluczowe. Pamiętaj jednak, aby zadać pytanie we właściwym czasie i miejscu. Najprawdopodobniej robienie tego, gdy czujesz się niekomfortowo, nie jest właściwym czasem i miejscem. W takiej sytuacji Twoje pytanie nie spowoduje bezstronnej i pozbawionej emocji odpowiedzi. Będzie się opierać na pragnieniach i uczuciach, a nie na danych i faktach. Rzuć wyzwanie decydentom, nie rzucaj wyzwania swojej karierze.

Jeśli nie możesz uzyskać dostępu lub jeśli drzwi są zamknięte, pozostań na zewnątrz

Każde środowisko IT będzie miało jakąś formę fizycznej i cyfrowej topologii obszarów o ograniczonym dostępie z selektywnym dostępem. Zasady te będą tworzone z biegiem czasu i często będą powiązane z historiami finansowymi, prawnymi i dotyczącymi bezpieczeństwa, których możesz nie znać – lub nawet nie wolno Ci poznać. Aby postępować etycznie, należy poznać i szanować te zasady. Należy założyć, że za ich realizacją stoją dobre intencje i rozsądna logika. Jeśli uważasz, że zasady utrudniają Twoją pracę, powinieneś skonsultować się ze swoim menadżerem i odpowiednimi właścicielami. Nie powinieneś próbować tworzyć własnych zasad.

Ograniczenia mają Cię chronić

„Jestem nowym pracownikiem. Nie daliby mi dostępu do tego rodzaju informacji.

Jest to polityka zalecana dla osób dopiero rozpoczynających pracę w firmie. Jako nowy pracownik powinieneś chronić się, nie uzyskując dostępu, którego nie wiesz, jak używać. Z biegiem czasu otrzymasz (lub zyskasz) dodatkowe uprawnienia i przywileje, gdy zapoznasz się z rolami i nabierzesz pewności w procedurach pracy.

„Zostawił telefon, a ja byłam przy nim przez cały czas".

W większości centrów danych obowiązują surowe zasady, które często zabraniają robienia zdjęć i często wymagana jest zawsze obecność upoważnionej eskorty. Taka praktyka pomaga zapobiec kradzieży, ale także zmniejsza ryzyko obrażeń i uszkodzeń. Elwood zadbał o przestrzeganie odpowiednich procedur – ale jak za chwilę omówimy, złamał także inne powiązane zasady.

Nie jesteś ponad „Prawem"

„Może powinienem był zainstalować w twoim systemie wygaszacz ekranu Bielefeld. Co byś chciał?"

Dowcip Friedy pojawia się w kontekście tego, że Wendell zostawia odblokowany komputer, co omówimy nieco później, ale jest to zły przykład etycznego zachowania. Technicznie rzecz biorąc, odblokowany komputer zapewnia jej dostęp, ale tak naprawdę nie ma żadnego uzasadnionego powodu, aby używać maszyny Wendella, nawet jeśli ma to na celu „zabawną" lekcję. Co więcej, rola Friedy jako specjalistki ds. bezpieczeństwa informacji stawia ją w niepewnej sytuacji. Ma uprawnienia

do przeprowadzania kontroli i audytów innych osób i systemów, ale jej obowiązkiem jest także pomaganie innym w zrozumieniu ich naruszeń i nauczeniu się, jak je prawidłowo rozwiązać.

„Byłem w łazience i minęło tylko kilka minut".

Z ludzkiego punktu widzenia sekundy lub minuty mogą trwać długo. W tym okresie komputery mogą wykonać tysiące, a może nawet miliony instrukcji. Wendell nie powinien posługiwać się „osobistymi usprawiedliwieniami" w celu naginania zasad.

„Muszę wiedzieć, na wypadek gdybyś ujawnił poufne dane!"

Żądanie Friedy leży w zakresie jej roli jako specjalisty ds. bezpieczeństwa informacji. Musi zrozumieć, czy doszło do jakichkolwiek szkód i jakie środki należy podjąć, aby je powstrzymać. Choć może się to wydawać przesadne, pomyśl tylko o tysiącach naruszeń bezpieczeństwa danych, które miały miejsce w ciągu ostatnich kilku lat, a wiele z nich doprowadziło do wycieku do Internetu prywatnych informacji i ton danych od setek milionów użytkowników.

„Więc dlaczego widziałem cię w centrum danych w sprawie bezpieczeństwa aby monitorować wczoraj? Bez wpisywania się do dziennika dostępu!"

Jest to dość poważne naruszenie procedur pracy, za które winni są zarówno Wendell, jak i Elwood. Elwood nie powinien był wpuszczać nikogo bez przestrzegania właściwej procedury. Stanowi to również zły przykład dla nowego pracownika, takiego jak Wendell, który może być bardziej skłonny do łamania zasad, widząc, jak jego „starsi" koledzy robią to samo. Ponieważ nie ma (jeszcze) dostępu, powinien trzymać się z dala od centrum danych lub postępować zgodnie z odpowiednią procedurą, aby uzyskać dostęp. Nawet jeśli Elwoodowi to nie przeszkadzało, Wendell powinien był zachować ostrożność – ponieważ w końcu (i słusznie) został obwiniony przez Friedę za to, co zrobił. Pamiętaj, że zasady mogą wydawać Ci się nudne lub bezsensowne, ale istnieją i dopóki nie zostaną zmienione (nawet poprzez Twoją własną interwencję i sugestie odpowiednim właścicielom), należy ich przestrzegać.

„Nie ma żadnych wycieczek po centrum danych. To bezpieczny obszar.

Nawet jeśli Wendell uzyskał dostęp, nie oznacza to, że może robić rzeczy zabronione przez zasady. Istnieje wiele powodów, dla których firmy nie zezwalają na wycieczki po centrach danych. Zwykle ma to na celu zapobieganie wyciekom adresów IP i kradzieży. Czasami obciążenia działające w systemach centrów danych mogą być tak wrażliwe lub krytyczne czasowo, że każdy błąd może spowodować znaczne szkody (wyobraź sobie gościa naciskającego przycisk na obudowie serwera). – Wciąż cię obserwuję. Firma powinna stawiać wymagania pracownikom, aby byli odpowiedzialni za siebie, a nie mieli nianię. Co więcej, zastraszanie nie działa jako niezawodny środek bezpieczeństwa na dłuższą metę.

Jeśli znajdziesz odblokowane „tylne drzwi", powiadom

Administratorzy systemów i technicy napotkają wiele bram w swojej przysłowiowej podróży IT. W związku z tym mają największe ryzyko natrafienia na błędne konfiguracje narzędzi i systemów. Jeśli odkryjesz lukę w zabezpieczeniach systemów, z którymi współpracujesz, powinieneś powiadomić odpowiednich właścicieli. Nawet jeśli nie jesteś w 100% pewien, że odkryłeś błąd lub problem w konfiguracji, powinieneś podkreślić swoje ustalenia, aby eksperci w danej dziedzinie mogli ocenić potencjalny problem i go rozwiązać. Tylnymi drzwiami może być wszystko, co umożliwia dowolny dostęp do uprzywilejowanych systemów lub ujawnienie poufnych danych. Może to być spowodowane luźnymi systemami bezpieczeństwa fizycznego, błędem oprogramowania, nieprawidłowymi

uprawnieniami, nieaktualną listą danych uwierzytelniających, słabymi hasłami lub uszkodzoną kamerą w korytarzu.

Reaguj szybko, gdy zostaną znalezione dziury

„Zostawiłeś komputer odblokowany!"

Komentarz Friedy może wydawać się ostry, ale działała w najlepszym interesie zarówno Wendella, jak i firmy. Jeśli pozostawisz ekran odblokowany, inne osoby będą miały nieograniczony dostęp do Twojego systemu i będą mogły zdecydować się na wprowadzenie zmian w Twoich plikach. Obejmuje to niewinne żarty, podczas których wysyłasz e-mail do całej firmy, zapraszając ludzi na darmową pizzę (wszyscy to robiliśmy, cóż, większość z nas), po złowrogie działania, takie jak przeglądanie lub kradzież czyichś prywatnych informacji – konta bankowego , ocena roczna i tak dalej. Wtedy druga osoba może również wykorzystać Twoją stację roboczą do kradzieży własności intelektualnej, danych klientów lub haseł do wrażliwych systemów. Jeśli takie naruszenie zostanie wykryte, zostanie ono powiązane z Twoim kontem i najprawdopodobniej zostaniesz pociągnięty do odpowiedzialności. Frieda należycie poinformowała Wendella o jego nieszczęściu i prawdopodobnie zapobiegła niepożądanemu dostępowi do jego komputera. Wendell szybko pochylił się i zablokował ekran komputera. Przynajmniej Wendell zareagował szybko i zatkał „dziurę". Nie jest to idealny scenariusz, ale jego działanie uniemożliwiło Friedie dostęp do jego maszyny.

Pozostawienie otwartych drzwi

„I jesteś zalogowany jako root… na więcej niż jednym terminalu."

Dowiedzieliśmy się, jak ważna jest separacja i najmniejsze przywileje. Korzystanie z konta z najwyższymi uprawnieniami administracyjnymi może czasami być konieczne, ale często tak nie jest. Trzymanie wielu aplikacji (w tym przypadku powłok w oknach terminala) otwartych i zalogowanego użytkownika root może stworzyć zagrożenie bezpieczeństwa, zwłaszcza że Wendell zostawił swój komputer odblokowany. Umożliwia to niekwestionowany dostęp do wszelkich danych, narzędzi i systemów, którymi dysponuje Wendell. Po raz kolejny krytyka Friedy jest uzasadniona, ponieważ Wendell rzeczywiście naruszył podstawowe zasady bezpiecznej pracy z kontami uprzywilejowanymi. Powinien był wykonać tylko jedno uprzywilejowane zadanie na raz, a następnie wylogować się po zakończeniu pracy.

„Nigdy nie wiadomo, do jakiego rodzaju danych ma dostęp serwer testowy. Każdy mógł skopiować pliki klientów."

Jest to rzeczywiście prawdopodobny wynik scenariusza „tylnymi drzwiami" do środowiska IT. Niezależnie od tego, czy zostały otwarte celowo (złośliwość lub włamanie), czy przez pomyłkę, tylne drzwi umożliwiają dowolny dostęp do systemów i danych. Możliwe, że serwer testowy Wendella jest odizolowany od środowiska produkcyjnego, ale mogą wystąpić problemy i błędne konfiguracje, o których Wendell nie jest świadomy, zwłaszcza gdy działa na koncie uprzywilejowanym.

„Przypomniał sobie również, że widział jedną z otwartych konsol, pokazującą na ekranie pewne dane".

Wendell powinien był powiadomić o tym Elwooda. Możliwe, że jeden z techników centrum danych przypadkowo zostawił otwartą konsolę. Mimo że jest to obszar zastrzeżony, użytkownik powinien po zakończeniu pracy wylogować się z serwera.

Ochrona środowiska IT i Ciebie

W idealnym świecie nie byłoby potrzeby żadnego bezpieczeństwa, a praca zawsze byłaby wykonywana w oparciu o zaufanie i najwyższą osobistą odpowiedzialność. Niestety, w prawdziwym świecie nie jest to możliwe. Nawet jeśli nie ma złych zamiarów, ludzie popełniają błędy. Omówiliśmy to w Rozdziale 1 (Oddzielne role), gdzie błędy i szkody mogą być spowodowane złym osądem, niewystarczającymi informacjami oraz brakiem procedur i umiejętności. Dobrze zaprojektowane środowisko IT zmniejsza ryzyko niepożądanego dostępu na wszystkich poziomach, począwszy od bezpieczeństwa fizycznego, poprzez dostęp do systemu oprogramowania, a skończywszy na dostępie uprzywilejowanym. Obejmuje to:

• Ograniczenia dostępu fizycznego – środowiska IT powinny być wyposażone w solidne mechanizmy zapobiegające przypadkowemu dostępowi, infiltracji i próbom ich ominięcia metodą brute-force. Mechanizmy te są zbudowane tak, aby były tolerancyjne i zapewniały niski odsetek fałszywych alarmów — jeśli systemy powodują więcej błędów niż uzasadnionych alertów (jak w przypadku chłopca, który krzyczał „wilk”), ludzie mają tendencję do ich ignorowania i stają się bezużyteczne.

• Ograniczenia dostępu do sieci – równolegle do systemów fizycznych, środowiska IT powinny być również chronione przed atakami i włamaniami opartymi na oprogramowaniu. Nastąpi separacja i izolacja cyfrowych enklaw, często w oparciu o wrażliwość danych, które zawierają, i poziom wymaganych przez nie uprawnień. Narzędzia ograniczania dostępu do sieci obejmują zapory ogniowe, skanery ruchu, detektory zachowań heurystycznych, listy kontroli dostępu i inne.

• Dostęp do tożsamości – muszą istnieć systemy, zarówno fizyczne, jak i cyfrowe, które będą kwestionować tożsamość w przypadku każdej próby dostępu do miejsc, w których obowiązują ograniczenia. Jeżeli dana osoba nie jest w stanie sprostać wyzwaniu, nie zostanie wpuszczona

• Jasne procesy – każdy (pracownicy, wykonawcy na miejscu, goście i goście) powinien móc szybko i łatwo zrozumieć, dokąd może się udać, jakie obowiązują ograniczenia i zasady oraz co zrobić, jeśli istniejąca konfiguracja nie będzie działać. pozwolić im dokończyć swoją pracę.

• Monitoring – W środowisku informatycznym powinno znajdować się narzędzie, które będzie odpytywać mechanizmy ograniczania dostępu. Narzędzia monitorujące będą miały progi, które pozwolą zautomatyzowanym systemom i operatorom identyfikować interesujące punkty danych, w tym incydenty, nietypowe zachowania, potencjalne naruszenia bezpieczeństwa i inne.

• Rejestrowanie — należy rejestrować dostęp (zarówno sukces, jak i niepowodzenie), ponieważ zapewnia on zapis działań wyjaśniający, w jaki sposób i kiedy używany był sprzęt. W idealnym przypadku przechowujesz je w bazie danych ze stałymi aktualizacjami, które prawidłowo odzwierciedlają bieżący stan uprawnień.

• Audyty – Baza danych powinna być okresowo kontrolowana pod kątem jakichkolwiek rozbieżności. Jeśli zostanie zaprojektowany prawidłowo, stanowi część szerszego systemu monitorowania i w razie potrzeby zapewnia również dowody kryminalistyczne.

• Alerty – systemy w środowisku IT powinny mieć jasne reguły, które zawsze zapewniają deterministyczną odpowiedź na każde żądanie dostępu. Pomyślne wpisy są rejestrowane. Wpisy zakończone niepowodzeniem są rejestrowane i, pod pewnymi warunkami, zgłaszane jako alerty, które można następnie dalej przetwarzać i analizować. Alerty powinny obejmować zrozumiałe procedury, dzięki którym ludzie będą wiedzieć, co robić i jak reagować na alerty, szczególnie w sytuacjach awaryjnych.

Dzięki temu będzie mniej przypadków przypadkowych naruszeń zasad dostępu przez pracowników, a ciekawscy ludzie będą mieli mniej możliwości decydowania się na włóczenie się, sondowanie i testowanie granic swojego środowiska pracy. Jednakże żaden proces nie jest w 100% niezawodny, a to przykazanie jest konieczne, aby w przypadku załamania się procesów ludzie nadal robili to, co jest etycznie słuszne.

Dostęp fizyczny

Trzymanie ludzi z dala od obszarów o ograniczonym dostępie służy wielu celom. Wcześniej krótko wspomnieliśmy o szpiegostwie przemysłowym i kradzieży. Dodatkowo bezpieczeństwo fizyczne ma na celu zapewnienie bezpiecznego środowiska pracy, do którego dostęp ma wyłącznie wykwalifikowany personel. Jest to prawie oczywiste, jeśli pomyślisz o wojsku, szpitalach, a może elektrowniach; Jednak większość ludzi niekoniecznie postrzega przytulne, dobrze wyposażone biura IT jako coś, co wymaga specjalnych środków. Istnieje kilka głównych powodów, dla których należy ograniczyć dostęp fizyczny:

• Bezpieczeństwo – środowiska IT niosą ze sobą niebezpieczeństwa. Typowe centrum danych to hałaśliwe miejsce, w którym znajduje się ciężki sprzęt, wysokie napięcie i prawdopodobnie otwarta podłoga. Osoby pracujące w tych obszarach są przeszkolone do pracy z określonym poziomem ryzyka zawodowego i rozpoznawania potencjalnych zagrożeń.

• Koszt – Ogólnie rzecz biorąc, ochrona przed zagrożeniami wewnętrznymi jest droższa i bardziej złożona niż zagrożenia zewnętrzne. O ile stosunkowo łatwo jest określić, kto należy do murów firmy, a kto nie, w obrębie organizacji znacznie trudniej jest podejmować proste, jednoznaczne decyzje. Im szybciej wykryjesz naruszenie lub wtargnięcie, tym taniej będzie zaradzić problemowi

• Przestępczość – Kradzież sprzętu jest wynikiem ludzkiej natury i możliwości. Chociaż nie da się zmienić ludzi, możesz stworzyć środowisko IT, które odstraszy od kradzieży. W Rozdziale 5 (Nie kradnij komputerów) mówiliśmy o cyklu życia sprzętu, monitorowaniu i znakowaniu, a wszystko to może pomóc w ograniczeniu strat materialnych.

W jednym z moich poprzednich miejsc pracy lokalne centrum danych miało naprawdę sprytną funkcję bezpieczeństwa. Wejście do hali centrum danych prowadziło przez obrotową, dwudrzwiową bramę, w której znajdowały się obciążniki. Po wejściu osoba zostanie zważona i powiązana z wartością karty dostępu. Jeśli przy wyjściu różnica w wadze wynosiła zaledwie 100 gramów (3 uncje), osoba była zamykana w cylindrycznej bramie, co natychmiast powiadamiało ochronę budynku i kierownika centrum danych. Zapobiegło to nieautoryzowanemu przenoszeniu wrażliwego lub ważnego sprzętu centrum danych (takiego jak dyski twarde). W przypadku konieczności przeprowadzenia skomplikowanej konserwacji, wymagającej częstego wjazdu i przemieszczania serwerów, brama była wyłączana i wysyłana na miejsce ochrona. Powyższy przykład może wydawać się ekstremalny, ale jest znacznie bezpieczniejszy niż podobne drzwi obrotowe w innym miejscu pracy, które nie miało podkładek obciążających, a jedynie stopkę dociskową o wymiarach 1 × 1. Gra polegała na sprawdzeniu, ile osób zmieści się w szklanym cylindrze, utrzymując cały ciężar na podkładce dociskowej. Nawet odwiedzający nas dostawca konserwacji sprzętu wziął udział w grze.

Granice fizyczne pomagają tworzyć bezpieczniejsze środowisko pracy. Jednak równie ważne jest, aby pamiętać, że ludzie zawsze będą szukać i znajdować sposoby na ich obejście. W pewnym momencie staje się to grą o malejących zyskach. Zamiast tego wzmocnienie etyki jest ostatnią (ale najskuteczniejszą) linią obrony.

Dostęp do oprogramowania

Istnieje wiele warstw sposobu, w jaki można i należy wdrażać zabezpieczenia oprogramowania. Chociaż szczegółowe szczegóły różnią się w zależności od środowiska IT, podstawowe zasady pozostają niezmienione. Większość z nich omówiliśmy wcześniej – a także w sekcji „Dostęp fizyczny” – i razem tworzą one warstwowy stos, który zapewnia niezbędne ramy dla bezpiecznej pracy.

• Rozdzielenie ról zmniejsza ryzyko szkód.

• Zarządzanie kontami umożliwia właścicielowi środowiska dostosowanie dostępu w oparciu o tożsamość i potrzebę wiedzy.

• Zarządzanie danymi pomaga zapobiegać incydentom związanym z naruszeniem prywatności.

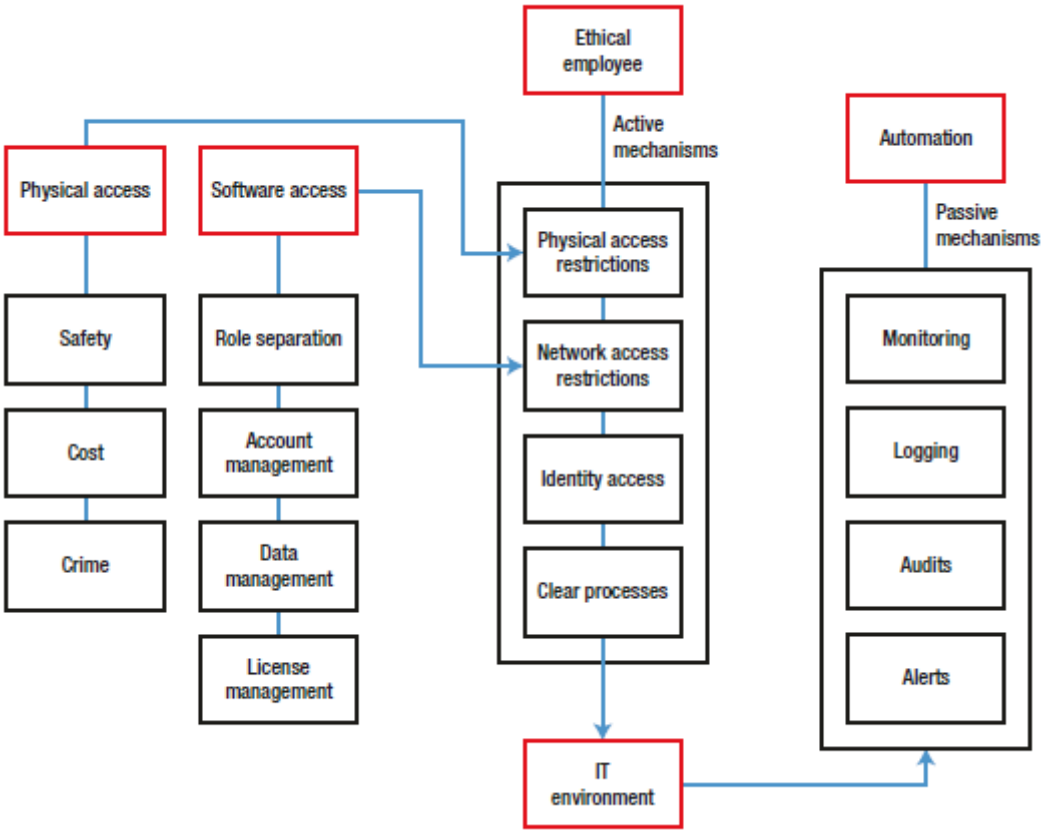
• Zarządzanie licencjami pomaga zapobiegać naruszeniom własności intelektualnej.

• Jasne i dokładne procesy dotyczą oprogramowania tak samo jak sprzętu.

• Automatyzacja ogranicza błędy wdrażania i zmiany konfiguracji.

• Monitorowanie, rejestrowanie, audyty i alerty zapewniają dokładny obraz bieżącego stanu środowiska, w tym praw dostępu i uprawnień do wszystkich istotnych funkcji.

Pełną konfigurację środowiska IT, obejmującą zarówno scenariusze dostępu fizycznego, jak i programowego, pokazano na rysunku



Biała lista a czarna lista

Im więcej zestawów reguł i reguł ma system, tym większe ryzyko fałszywie pozytywnego wyniku. Skuteczne systemy bezpieczeństwa zakładają domyślne podejście odmowy, w którym wszelki dostęp

jest zabroniony każdemu i wprowadzane są częściowe wyjątki (w oparciu o tożsamość i funkcję). Dotyczy to zarówno narzędzi fizycznych, jak i cyfrowych (oprogramowania).

Testy penetracyjne

Niezależnie od tego, jak kusi Cię (i sprytność), nigdy nie powinieneś samodzielnie próbować łamać, wzmacniać ani testować swojego środowiska IT. Testy penetracyjne to popularna metoda oceny jakości, odporności i skuteczności mechanizmu bezpieczeństwa. Na przykład sieć informatyczna jest poddawana serii skoordynowanych, zautomatyzowanych ataków, a wyniki są analizowane w celu ustalenia, jakie jest prawdopodobieństwo, że sieć wytrzyma prawdziwy atak z zewnątrz. Metody mogą obejmować określone min-pułapki przeglądarki, wyliczanie usług, hakowanie routerów i zapór sieciowych metodą brute-force, odmowę usługi (DoS), rozproszoną odmowę usługi (DDoS), exploity dnia zerowego i inne ładunki. Zazwyczaj testy te przeprowadza firma zewnętrzna, za zgodą działu bezpieczeństwa informacji. Możesz zdecydować, że masz podobne umiejętności i wiedzę i chcieć przeprowadzić te testy samodzielnie. Zwykle, jeśli podejmowane są bez zezwolenia, takie próby skutkują wszczęciem postępowania dyscyplinarnego, a nawet zwolnieniem. Być może Twoja wiedza techniczna może zostać dobrze wykorzystana, ale wszelkie testy systemów bezpieczeństwa muszą zostać zatwierdzone. Nawet w przestrzeni osobistej, w chmurze, musisz poprosić dostawcę chmury o autoryzację na przeprowadzenie testów penetracyjnych. W przeciwnym razie nie można go odróżnić od ataków, które prawie zawsze są klasyfikowane jako działalność przestępcza. Jeden dobrze udokumentowany przypadek przeprowadzenia przez administratora systemu nieautoryzowanych testów penetracyjnych miał miejsce w naszym poprzednim miejscu pracy. Popularny autor informacji technicznych i szanowany konsultant, Randal Schwartz znany również jako Merlyn, aktywnie uruchomił narzędzie penetracyjne Crack na skrótach haseł. Kiedy dowiedział się, że ktoś zhakował jego osobistego dostawcę usług internetowych, chciał mieć pewność, że to samo nie przydarzy się w firmie Intel Corporation, gdzie pracował w laboratorium na zlecenie. Crack ujawnił 2 z 30 haseł w laboratorium, w którym pracował. Następnie użył jednego z tych haseł, aby uzyskać dostęp do skrótów haseł na głównym serwerze poza laboratorium. Ponieważ jego sesja Crack trwała kilka dni na głównym serwerze, jeden z administratorów serwera zauważył tę sesję i zgłosił ją ochronie. W następnym tygodniu policja przyszła do jego domu z nakazem przeszukania i skonfiskowała cały sprzęt komputerowy. Randal został ostatecznie postawiony przed sądem za modyfikowanie komputera bez zezwolenia, co stanowi przestępstwo w świetle prawa stanu Oregon.

Wniosek

Ten sam rodzaj ciekawości, który popycha ludzi o technicznych poglądach do wielkich osiągnięć i wynalazków, działa również przeciwko nim, gdy rzucają im wyzwanie autorytety i pozornie arbitralne granice. Ta walka pomiędzy osiągnięciem za wszelką cenę a granicami wyznaczonymi przez władze jest powszechna w miejscu pracy; mamy tendencję do walki o naszą „wolność". Ale walka stawia nas również w trudnej sytuacji, ponieważ łatwo możemy dopuścić się naruszeń etyki. Należy przestrzegać ograniczeń, nawet jeśli nie od razu rozumiemy całą historię lub uzasadnienie tych ograniczeń. Dotyczy to w równym stopniu dostępu fizycznego, jak i cyfrowego (oprogramowania). Kiedy trafisz na coś, co wydaje się nieuzasadnionym ograniczeniem, przekaż swoje obawy właścicielowi polisy. Jeśli to Ty jesteś osobą, której obowiązki zawodowe obejmują projektowanie i utrzymywanie systemów ograniczających dostęp, pomyśl o idealnym modelu jak o cebuli – warstwa po warstwie zabezpieczeń, której koszty i ryzyko rosną w miarę ich usuwania. Twoje systemy powinny być solidne, tolerancyjne, dokładne i zapewniać łatwy ślad dowodowy. Środowisko zostało zaprojektowane tak, aby było przejrzyste, więc nie zakłócało pracy i rutyny ludzi – co tylko zwiększa ryzyko naruszeń. Następnie, jeśli coś pójdzie nie tak, twój ślad dowodu pomoże ci zrozumieć i naprawić problemy, a także wszelkie luki w twojej obronie. Na koniec należy pamiętać, że mechanizmy bezpieczeństwa mogą niewiele. Ogólnie

rzecz biorąc, to przestrzeganie pierwszych pięciu przykazań pomaga skutecznie skleić stos. Mimo najlepszych intencji i większości narzędzi, czasami coś pójdzie nie tak. To tylko kwestia czasu – i pewnych skomplikowanych prawdopodobieństw. Ważne, a nawet kluczowe jest posiadanie odpowiednich narzędzi i systemów oraz postępowanie etyczne. Podobnie trzeba wiedzieć, jak się zachować, gdy sprawy nagle przybierają zły obrót. Odejdziemy od scenariuszy z czasów pokoju i porozmawiamy o etycznym zachowaniu w obliczu niepewności. Zaczniemy od siódmego przykazania – Postępuj zgodnie z procedurami i uciekaj.