Oddzielne role

Wendell wrócił myślami do swoich interakcji z każdym z członków zespołu. Czy coś, co zrobili, mogło przyczynić się do wyłomu? Może jego obecność wywołała wydarzenia, które doprowadziły do wyłomu. Pierwsze dni w nowym miejscu pracy przypominają wizytę w nowym mieście. Jesteś turystą i najprawdopodobniej w lekkim szoku, najlepiej przyjemnym. Nie wiesz do końca, co robić - nawet jeśli robiłeś to wcześniej - i szukasz renomowanego źródła mądrości, które pomoże ci się poruszać. Dla Wendella przewodnikiem turystycznym był Alex i od razu wiedział, że powinien stąpać delikatnie.

„Masz szczęście" - udramatyzował Alex.

"Oh?"

„Zwykle poczekałbym kilka tygodni, zanim przyznałbym ci prawa dostępu, ale Mike'owi zależy na jak najszybszym włączeniu cię na pokład, więc robimy wersję przyspieszoną. Pracowałeś już wcześniej z kontami uprzywilejowanymi?

Wendell skinął głową.

"W porządku. Więc tak to działa. Twoim standardowym użytkownikiem jest Wendell i teraz skonfigurujemy wendell_p. To będzie twoje konto użytkownika zaawansowanego i będziesz go używać do uprzywilejowanego dostępu. Nie używasz do tego swojego zwykłego konta, używasz tego.

„Czy to jest konto sudo?" Wendell próbował wykazać się wiedzą. Alex pomachał niecierpliwie. „Właściwie to pięć kont".

Wendell zaśmiał się cicho. "Pięć? Na moim ostatnim miejscu używaliśmy tylko na jednym. Cóż, dwóch. Mieliśmy standardowe konto do prawie wszystkiego i rootowanie, gdy musieliśmy wykonać pewne prace administracyjne na serwerach".

Alex zamrugał. Wyglądało na to, że nie lubił, gdy przerywano mu występ. „Oddzielne konta to mądra rzecz. Po pierwsze, zapewniają większą szczegółowość, jeśli chodzi o pracę. Po drugie, minimalizują ryzyko. Po trzecie, wyraźnie wiesz, co robi każde konto i do czego jest używane. Teraz wszystko jest powiązane z Twoim użytkownikiem, ale jest mapowane na pięć systemów zarządzania użytkownikami. Po pierwsze, jeśli chcesz pracować na komputerach z systemem Windows, będziesz mieć konto AD. Potem jest też wysokie konto. To jest uprzywilejowane konto do administrowania systemem Windows". Alex przerwał, żeby spojrzeć na coś na ekranie swojego telefonu. „Czy wiesz, co to jest zarządzanie dostępem uprzywilejowanym?" Wendell ponownie skinął głową. „Masz na myśli narzędzia PAM?" "TAK". Dobrze. Ponieważ będziemy musieli skonfigurować Ci dostęp SSH, abyś mógł wykonywać administrację zdalną. Teraz łączysz się z własnym kontem przez SSH do innych systemów, a następnie przełączasz się na wendell_p tam. Zgodnie z polityką nie zezwalamy użytkownikom _p na SSH do innych hostów".

Rozumiem - powiedział Wendell, wściekle zapisując notatki. Alex odwrócił krzesło z powrotem do biurka i zaczął pisać oraz uruchamiać polecenia, szybciej, niż by sobie tego życzył Wendell, ale to była sprawa Alexa i postanowił nie przerywać.

„Teraz... konto użytkownika zaawansowanego jest dobre i dobre, ale czasami potrzebujesz odpowiedniego roota". Alex napisał coś na kartce papieru. Był to ciąg składający się z ośmiu liter i Wendell założył, że jest to hasło. „To jest nasze obecne hasło roota. Teraz normalnie przechodzisz do trybu online, aby uzyskać hasło. Pokażę ci. Tutaj. Przejdź do kont ukośnych; które przekierują do naszego internetowego systemu zarządzania hasłami. Nazywa się Sesame i jak widać, to brzydka rzecz zaprojektowana w minionym tysiącleciu. Tutaj logujesz się za pomocą swojego zaawansowanego

użytkownika. A następnie kliknij Poproś o hasło roota, a wyświetli się hasło na ekranie przez 30 sekund. Więc jeśli go zapomnisz lub hasło się zmieni, zawsze możesz je zdobyć w ten sposób". Alex podniósł palec. „Tylko z lokalnym adresem IP. Nie będzie działać przez VPN". Wendell podkreślił w swoim notatniku alias intranetowy. "Zrozumiane." "Doskonale. A teraz napijmy się kawy, jadę na oparach.", Nie czekając, aż Wendell rzeczywiście odpowie, Alex pobiegł do kawiarni, machając swoim starym kubkiem z wyblakłym logo jak pałką. Po drodze zatrzymał się, aby zamienić kilka starych i niezbyt śmiesznych dowcipów z ludźmi siedzącymi przy innych biurkach. Wendell tak naprawdę nie uchwycił wewnętrznego znaczenia większości z nich. Uważał, że było to dobrze praktykowane i często powtarzany rytuał. Wróciwszy do biurka Alexa, Wendell przypomniał sobie prezentację pierwszego dnia w pracy, pozornie niekończący się strumień slajdów, sloganów i mini-wywiadów z tym czy innym kierownikiem. „A co z dostępem do VPN?" Alex pstryknął palcami. „To zadziała tylko z twojego służbowego laptopa. Teraz, w przeciwieństwie do Sesame, który działa tylko w sieci firmowej, nie można z niego korzystać z poziomu intranetu. Musisz być w Internecie, jak w domu lub w kawiarni. Ale pozwól, że pokażę ci coś fajnego." Alex odblokował telefon i uruchomił coś, co wyglądało jak aplikacja konsolowa, czarne tło i migający kursor.„Ustawiłem specjalny host bastionu w DC, który pozwala mi logować się z tego urządzenia". Wendell był ciekawy. Nie pamiętał też niczego o telefonach, o których wspominano nigdzie w celu uzyskania dostępu do systemu. „Używasz SSH do bastionu, a następnie przełączasz się na konto administratora?" "Tak. Oszczędza czas. Kiedy mam dyżur w nocy, a operatorzy dzwonią do mnie, o wiele łatwiej i szybciej jest po prostu od razu zalogować się przez telefon i zobaczyć, co się dzieje. Przez większość czasu są to po prostu błahe błędy w konfiguracji i mogę szybko naprawić problemy i zamknąć zgłoszenie. Ale jeśli muszę wykonać dużo pracy, włączam laptopa, włączam VPN i zajmuję się pełną parą". Wendell zacisnął usta. Uważał to za praktyczne, ale zastanawiał się nad modelem bezpieczeństwa. Postanowił jednak nie poruszać tego tematu. Alex znowu pisał. „Skoro jesteś nowy, jeśli nie masz pewności, to najlepiej zapytać. Teraz to dobrze znany fakt, że jeśli wykonujesz prace administracyjne, popełniasz błędy". Alex wstał, odsuwając krzesło. "Henry!" "Co tam?" „Ile razy przypadkowo zrestartowałeś serwer klienta?" „Za dużo" - mruknął Henry, zajęty za biurkiem. Alex usiadł. „Więc nie martw się tym. Ale pamiętaj. Z kontem zasilania i rootem możesz łatwo spowodować poważną awarię, więc dokładnie sprawdź swoje polecenia; a jeśli uruchamiasz skrypt na wielu hostach, zawsze poproś kogoś innego, aby to sprawdził, zanim naciśniesz Enter. Każdy w zespole zrobi to." Wendell skinął głową. „Więc to nie ma znaczenia kto?" „Wszyscy dotykamy prawie każdego aspektu administracji. Nie oznacza to, że każdy z nas jest ekspertem od wszystkiego, ale czasami jest to konieczne. Niedawno skonfigurowałem konto Belinda na wysokim koncie dostępu do danych klientów. Musiała przejrzeć niektóre dzienniki aplikacji, ponieważ jej klient skarżył się na problemy z wydajnością". Wendell pisał dalej w swoim notatniku. Zapowiadał się długi dzień.

ODDZIELNE ROLE

* Nie używaj uprzywilejowanego konta do pracy osobistej.

* Nie używaj uprzywilejowanego konta współdzielonego bez tożsamości logowania.

Dlaczego rozdzielanie ról jest ważne?

Zwrot „Wielka moc wiąże się z wielką odpowiedzialnością" jest powszechnie przypisywany Marvel Comics Amazing Fantasy #15 w 1962 roku, na długo przed tym, zanim administracja systemem oparta na oprogramowaniu stała się przedmiotem. Ale cytat, w takiej czy innej formie, został przypisany Winstonowi Churchillowi, Voltaire'owi, Williamowi Lambowi, a może nawet Biblii. Wydawałoby się, że przez wieki ludzie rozumieli moralny ciężar władzy. Przeskok wiary od rządu i filozofii do administracji systemu wydaje się raczej oderwany od implikacji, jakie niesie ten cytat, zwłaszcza że podstawowa różnica między zwykłymi użytkownikami a uprzywilejowanymi użytkownikami w systemie polega

jedynie na numerze identyfikacyjnym, który posiadają ich konta. Ale jest. Pozycja władzy pozwala ludziom wykorzystać tę moc i dokonywać zmian, których inni nie mogą dokonać, niezależnie od ich pragnień lub umiejętności. W świecie IT uprzywilejowane konta systemowe są najbardziej rozpowszechnionym interfejsem dla administratorów systemów, służącym do przekraczania granicy od zwykłego użytkowania, ograniczonego do osób i ich własnych danych, do szerszych działań, które mogą mieć wpływ na inne systemy – i z kolei na innych ludzi. Kiedy zatrzymasz się i pomyślisz, jedyną rzeczą, która naprawdę powstrzymuje uprzywilejowanych użytkowników przed spowodowaniem totalnego chaosu, jest ich osąd. Co zrobisz, jeśli źle osądzisz? Oczywiście powodujesz szkody. Na początku świata oprogramowania inżynierowie zdali sobie sprawę, że mogą łatwo paść ofiarą własnych słabości, kaprysów i uczciwych błędów oraz że muszą stworzyć zewnętrzne mechanizmy między subiektywnym rozumowaniem a twardymi danymi. W rezultacie zaprojektowano różne mechanizmy bezpieczeństwa, aby stworzyć wymuszony rozdział między zwykłym użytkowaniem (codzienną pracą, która jest unikalna dla każdej osoby, grupy lub projektu) a uprzywilejowaną pracą administracyjną (utrzymaniem systemów i usług, które umożliwiają ludziom wykonywanie ich codziennej pracy). . Najczęstszym przykładem oddzielenia uprzywilejowanego dostępu od wspólnego konta użytkownika jest konto użytkownika root w systemach UNIX/Linux. Dzięki tej separacji użytkownicy systemu mogą korzystać z aplikacji i usług bez możliwości wprowadzania zmian w bazowym systemie operacyjnym lub konfiguracji serwera. Ale ci, którzy mają dostęp do roota, mają możliwość wprowadzenia praktycznie dowolnych zmian w systemie, w tym usuwania dowodów własnej pracy (czyszczenie dzienników systemowych, wyłączanie rejestrowania, zmiana uprawnień itp.). Użytkownicy root mogą naprawdę zrobić wszystko, a ogólnie jest bardzo niewiele do zatrzymania polecenia roota od uruchomienia. Głównym problemem konta roota jest to, że może być tylko jedno (miłośnicy górali, radujcie się). Innymi słowy, jeśli ty lub ja pomyślnie uwierzytelnimy się jako użytkownik root, obaj jesteśmy użytkownikiem root. Nie ma między nami różnicy technicznej, a nasze polecenia będą przypisane do tego samego identyfikatora użytkownika. To sprawia, że root jest anonimowym współdzielonym kontem - tożsamość osoby logującej się nie jest wiarygodnie identyfikowalna. Konieczność wykonywania zadań administracyjnych - niezależnie od zwykłej pracy - oraz możliwość utrzymania pewnego poziomu identyfikacji w systemie doprowadziła do powstania mechanizmów przypominających rootowanie (jak popularne sudo w Linuksie czy Run As w Windows), które pozwalają czasowe przejście z ograniczonej, codziennej pracy do czynności uprzywilejowanych i poprawne zalogowanie takiej pracy w systemie. Wydawałoby się, że wszystkie zmartwienia i problemy związane z administracją systemem powinny były zostać rozwiązane przez wprowadzenie narzędzi przypominających rootowanie, prawda?

Cóż, nie do końca.

Wręcz przeciwnie.

Ponieważ coraz więcej osób otrzymało uprawnienia administracyjne, świat IT stworzył więcej punktów awarii w swojej strukturze. Co ważniejsze, żadne z narzędzi nie odnosi się do fundamentalnej kwestii etyki. Wszystko sprowadza się do posiadania odpowiednich danych uwierzytelniających - jeśli to zrobisz, uzyskasz dostęp.

Nie używaj konta uprzywilejowanego do pracy osobistej

Poświadczenia zapewniają dostęp - ale uprzywilejowany dostęp nie obejmuje z natury osądu etycznego. Ponieważ koncepcja etyczna każdej osoby jest różna - i zależy to od dostępnych danych, sytuacji, nastroju, koncentracji, zmęczenia, presji rówieśników, ograniczeń czasowych i odpowiedniego doświadczenia – ważne jest, aby celowo zminimalizować korzystanie z uprzywilejowanego dostępu, aby zminimalizować błędy . Ponieważ prawie niemożliwe jest uniknięcie wszystkich błędów, zdrową i

zalecaną praktyką jest używanie uprzywilejowanego dostępu tylko wtedy, gdy jest to absolutnie konieczne do wykonania zadania, a następnie ciągłe udoskonalanie procesów w celu zminimalizowania konieczności korzystania z uprzywilejowanego dostępu następnym razem. Ponadto istnieją różne zestawy zasad, zarówno technicznych, jak i biznesowych, dotyczących korzystania z konta osobistego i konta uprzywilejowanego. Na przykład możesz zdecydować się na usunięcie wszystkich plików i folderów ze swojego konta osobistego, ale zrobienie tego z uprzywilejowanym kontem naraziłoby system na szwank i wpłynęłoby na wszystkich użytkowników. W naszej historii Alex podkreślił znaczenie separacji kont i przejrzał listę różnych typów kont i uprawnień, które istniały w ich środowisku, a także mechanizmy żądania dostępu do konta root za pomocą portalu intranetowego. Alex poruszył również temat błędów i zarówno Henry jak i on otwarcie przyznali, że popełnili je w trakcie swojej pracy. Chociaż nie należy być „dumnym" ze swoich błędów, ważne jest, aby się nimi dzielić, aby ludzie mogli rozwinąć świadomość i dowiedzieć się o sytuacjach i warunkach, kiedy i gdzie te błędy się wydarzyły. W przypadku nowego pracownika, takiego jak Wendell, powinno to pomóc zaszczepić poczucie odpowiedzialności, zdrową dawkę podejmowania ryzyka i zrozumienie, że uczciwe błędy mogą i będą się zdarzać. Teraz, jeśli spojrzymy na to pod innym kątem, możemy też zobaczyć kilka braków w spotkaniu dwóch kolegów. Alex chciał jak najszybciej skonfigurować Wendella, co wskazuje na ograniczenia czasowe, które niekoniecznie pozwalają na spełnienie wszystkich istotnych kryteriów. Jednak takie „skróty" są często niebezpieczne, ponieważ stwarzają sytuacje, w których osoby o ograniczonej wiedzy lub znajomości środowiska IT mają uprzywilejowany dostęp. Przed przyznaniem (i zaakceptowaniem) takiego dostępu należało zweryfikować zrozumienie przez Wendella właściwego wykorzystania uprzywilejowanego dostępu na jego nowym stanowisku. Wendell powinien swobodnie wyrażać swoje obawy, niezależnie od tego, czy dotyczy to jego zaufania jako administratora systemu w zupełnie nowym środowisku, czy dzielenia się hasłami. Powinien swobodnie przerywać Alexowi, jeśli potrzebuje wyjaśnień, zwłaszcza że Alex pracował szybko, a Wendell musiał robić notatki podczas wykładu i demonstracji. W końcu spotkanie Alexa z Wendellem ma na celu zapoznanie nowego pracownika z procedurami i narzędziami stosowanymi w firmie. Jedynym skutecznym rezultatem jest skuteczne opanowanie domeny przez Wendella. Może to również oznaczać dokumentację dotyczącą procesu zarządzania kontem, wydrukowaną ściągawkę lub odniesienie do szkolenia online. Alex mógł zainicjować szkolenie w miejscu pracy (OJT), pozwalając Wendellowi na wpisywanie poleceń - i Wendell powinien był zadać to samo.

Nie używaj uprzywilejowanego konta współdzielonego bez tożsamości logowania

Istnieje kilka powodów, dla których warto rejestrować tożsamość podczas korzystania z uprzywilejowanego konta współdzielonego. Oczywistą odpowiedzią jest bezpieczeństwo informacji; jeśli i kiedy coś pójdzie nie tak, masz ślad kryminalistyczny. Mniej oczywistą odpowiedzią jest to, że zmniejsza to podejrzenie, gdy coś pójdzie nie tak. Na przestrzeni lat branża IT wypracowała silne i często niezbędne skupienie się na aspektach bezpieczeństwa, a wiele, jeśli nie wszystkie, uprzywilejowane działania są natychmiast kojarzone z tą dziedziną. Uprzywilejowane konto współdzielone nie jest świetną okazją do robienia rzeczy bez konsekwencji; wręcz przeciwnie, należy go traktować z maksymalną odpowiedzialnością i rozliczalnością. Ponadto praca z uprzywilejowanym kontem współdzielonym powinna być udokumentowana. W ten sposób zespół IT ma pełny dziennik wykonanej pracy i może kojarzyć działania z poszczególnymi osobami. Nie w celu obwiniania, ale w celu osiągnięcia jasności i porządku oraz zminimalizowania błędów. W naszej historii dotknęliśmy tylko konta root, ale zasada dotyczy wszystkich wspólnych kont tożsamości, takich jak bazy danych lub usługi aplikacji. Omówimy je w kolejnych sekcjach. Zapewniając dostęp do roota, Alex sprawił, że Wendell nie miał innego wyjścia, jak tylko naruszyć część pierwszego przykazania dotyczącą wspólnego konta (nie używaj uprzywilejowanego konta współdzielonego bez logowania tożsamości). Wendell otrzymał dostęp do roota, ale nie otrzymał instrukcji dotyczących mechanizmów logowania tożsamości podczas

jego używania. Wendell miał swoje zastrzeżenia i powinien był zgłosić je Alexowi. Wendell miał przecież doświadczenie z poprzedniego miejsca pracy, a jego wkład mógł być cenny. Jeśli Wendell uważał, że niektóre sugestie Alexa nie są idealne, można je ulepszyć lub potencjalnie wprowadzić ryzyko do firmy, powinien to powiedzieć. Współpraca między członkami zespołu to świetny sposób na budowanie zaufania - oraz poprawę jakości zarówno środowiska pracy, jak i wykorzystywanych narzędzi technicznych. Wendell mógłby przekazać swoje sugestie Alexowi. Jeśli nie czuł się komfortowo robiąc to na miejscu, mógł sporządzić listę i zaprezentować ją na następnym spotkaniu zespołu lub wysłać e-mail do zespołu, aby zobaczyć, co myślą o jego pomysłach. Na dłuższą metę otwarta dyskusja prawie zawsze prowadzi do udoskonalenia istniejących procedur. Ponadto korzystanie z osobistego bastionu do pracy dyżurnej jest kolejnym wykroczeniem. Jest to sprzeczne z ósmym przykazaniem (komunikuj zmianę), ponieważ Alex stworzył układ, który nie był udokumentowany jako formalny proces pracy, a także dziewiąte przykazanie (nie szkodzić), ponieważ miał uprzywilejowany dostęp do sieci „tylnymi drzwiami" ze swojego telefon narusza procedury pracy i pozwala Alexowi wyrządzić szkody w niespotykany i nieoczekiwany sposób

Procesy wspierające zachowania etyczne

Jest kilka rzeczy, które zespoły administracyjne mogą wykorzystać do ułatwienia etycznego zachowania, zwłaszcza jeśli chodzi o dostęp uprzywilejowany.

Transfer wiedzy

Jednym z najważniejszych kroków w procesie rekrutacji nowych pracowników jest skuteczny program onboardingowy, który pomaga ludziom szybko i bez dwuznaczności poznać swoje role i obowiązki. W zespole Wendella odbył się zorganizowany transfer wiedzy. Alex chciał podzielić się swoim doświadczeniem z nowym pracownikiem i pomóc mu wejść na pokład. Alex omówił różne rodzaje kont i ich przeznaczenie oraz podkreślił ważne aspekty tego, kiedy i jak z nich korzystać. Zademonstrował również niektóre przykłady, aby Wendell mógł być świadkiem rzeczywistej pracy. Jest też miejsce na ulepszenia. Na przykład Alex mógłby uzupełnić swoje ustne wyjaśnienie pisemnym dokumentem, aby Wendell mógł wrócić i odnieść się do niego w razie potrzeby. Może to również pomóc w wyjaśnieniu wszelkich terminów lub poleceń, które Wendell mógł pominąć. Wendell słuchał uważnie, zadawał pytania i robił notatki. Wendell wykazywał zainteresowanie nauczaniem swojego kolegi i prosił o wyjaśnienia, gdy nie był do końca pewien w określonym temacie. Podobnie jak Alex, Wendell może również sprawić, że sesja edukacyjna będzie bardziej efektywna. Mógłby nalegać na uzyskanie wszystkich odpowiedzi i przykładów, których potrzebuje, aby czuć się pewnie w wykonywaniu swoich obowiązków. Powinien również uważać, aby nie narazić się na uprzywilejowany dostęp lub nie pozwolić sobie na ujawnienie, przyjmując w „ciemnym zaułku" kawałek papieru, którego nie potrzebuje do wykonywania swojej pracy. Nowy pracownik, taki jak Wendell, powinien oczywiście agresywnie podchodzić do uczenia się i robienia nowych rzeczy, ale także do etyki i ograniczania ekspozycji. Nie powinien ułatwiać swojemu nauczycielowi.

Procedury pracy

Pamięć ludzka to niezwykła rzecz, ale może też być kapryśna i płatać nam figle. Mamy w głowach ogromną ilość wiedzy, ale czasami potrzebujemy prostej jasności, zwłaszcza jeśli chodzi o pracę wysokiego ryzyka. Najprostszym sposobem na zapewnienie, że procedury pracy są przestrzegane w przewidywalny, powtarzalny i jednolity sposób, jest dokładne dokumentowanie procesów pracy, tak aby każdy mógł odnieść się do odpowiednich informacji i móc wykonywać pracę tak samo wydajnie i poprawnie, jak jego koledzy . Nie usuwa to potrzeby umiejętności rozwiązywania problemów, innowacji lub zdrowego rozsądku - daleko od tego - ale musi istnieć punkt odniesienia, wspólny język, do którego każdy może się kierować i do którego można się odwoływać. Alex dysponował pełnym

zestawem procedur i poleceń, które mógł następnie zademonstrować Wendellowi. Przeanalizował również każdy rodzaj kont i wyjaśnił ich użycie, cel i scenariusze, kiedy ich użycie jest wymagane, ale co równie ważne, kiedy nie jest. Kontynuacją spotkania może być dokument pisemny. Wendell rozumiał, jak ważne jest przestrzeganie zasad, i poprosił nawet o wyjaśnienia, gdy uważał, że niektóre przykłady Alexa mogą nie być w pełni zgodne z procedurami.

Ćwicz

Procedurom pracy musi towarzyszyć praca praktyczna. Daje to pewność siebie i pozwala wszystkim zaangażowanym sprawdzić, czy lekcje są realizowane we właściwy sposób. Alex poświęcił czas na pokazanie poleceń. Jest to bardzo pomocne, ponieważ pokazuje rzeczywistą pracę i pomaga budować pewność siebie. Sesja byłaby jeszcze bardziej efektywna, gdyby Wendell również użył komputera i uruchomił te same polecenia po raz drugi. Kolejnym doskonałym punktem prezentacji Alexa jest skonsultowanie się z jednym z członków zespołu podczas uruchamiania skryptów i wrażliwych poleceń na wielu hostach. Pomaga to zredukować błędy i budować relacje.

Zachowania, które powstrzymują etykę

Podobnie jak w przypadku procesów wspierających zachowania etyczne, istnieją pewne negatywne cechy, które mogą ułatwiać łamanie zasad etyki w miejscu pracy. Mogą one przejawiać się na poziomie indywidualnym lub zespołowym, a nawet stanowić część szerszej kultury organizacyjnej. Jednak często zaczyna się od osoby.

Zbytnia pewność siebie

Alex jest całkiem pewny siebie. Jego poczucie pewności siebie wpaja poczucie słuszności (w jego działaniach), które inni ludzie mogą pomylić z ratyfikowaną polityką pracy. Z nowym pracownikiem, takim jak Wendell, może to od samego początku stworzyć wypaczone poczucie odpowiedzialności. Rodzi niewłaściwy rodzaj kultury pracy.

Niezgodność i nieufność

Zachowanie Alexa ma również wpływ na procedury pracy. Jeśli ludzie nie będą ich przestrzegać, może to prowadzić do większej liczby błędów, a tym samym do dalszych szkód, co spowoduje obciążenie administratorów systemu. Jeśli istniejące procedury i narzędzia okażą się niewystarczające (niezależnie od tego, w jaki sposób są używane lub omijane) w oferowaniu stabilnego środowiska pracy, kierownictwo firmy prawdopodobnie będzie zmuszone do wdrożenia dodatkowych procedur i narzędzi, aby spróbować ograniczyć przyszłe problemy i szkody. Takie zmiany mogą mieć dodatkowe konsekwencje i omówimy je później. Jak wielkość i skład mojego zespołu administracyjnego systemu , ewoluowali klienci i serwery, ewoluowały również metody, których używałem do zmiany haseł kont współdzielonych, przede wszystkim konta root. Gdy zespół liczył około pięciu osób i obsługiwał lokalne serwery, ręczne zainicjowanie zmiany było wystarczające. Wraz ze wzrostem zespołu i liczby obsługiwanych serwerów konieczna była automatyzacja w celu zainicjowania regularnej zmiany hasła i bezpiecznego przechowywania hasła. Gdy scentralizowane grupy usług potrzebowały dostępu do kont uprzywilejowanych (w tym hasła root), dodaliśmy możliwość szybkiej zmiany hasła, gdy pracownik opuścił firmę lub przeniósł zespoły. Wsparcie dwadzieścia cztery na siedem z zespołów z całego świata stworzyło potrzebę zezwolenia na „sprawdzenie" hasła roota tylko z wymaganym komentarzem, dlaczego hasło było potrzebne. Kultura polegała na rozwijaniu procesów, które nie wymagały hasła roota ze względu na to, że dokonano „zamówienia". Zmiana hasła root pomaga wzmocnić kulturę ograniczania korzystania z kont współdzielonych i zwiększania rejestrowania tożsamości, gdy konieczne jest użycie konta współdzielonego. Posiadanie jasnych danych, które pokazują, kto zna hasło

roota, nie tylko chroni firmę przed złym aktorem, ale także chroni każdego, kto może mieć dostęp do roota. Były pracownik, nowy pracownik, osoba na drugim końcu świata – to ludzie, których obwinia się, gdy dochodzi do błędów lub rażącego sabotażu. Zmiana hasła zaraz po odejściu i podawanie hasła tylko wtedy, gdy jest potrzebne, znacznie ogranicza liczbę osób, które muszą wziąć udział w dyskusji, gdy uprzywilejowany dostęp zostanie zidentyfikowany jako przyczyna problemu ze środowiskiem komputerowym. W historii Wendella natychmiast stał się możliwą przyczyną włamania, gdy otrzymał napisane hasło roota, nawet jeśli nigdy go nie używał. Istnieje kilka problemów etycznych związanych z pracą Alexa, oprócz stosu technologii i bezpieczeństwa. Korzystanie z dyżurnego hosta bastionu jest przede wszystkim naruszeniem czwartego przykazania (Nie idź tam, gdzie nie jesteś chciany). Alex powinien przestrzegać tych samych wytycznych dotyczących pracy, co wszyscy inni, gdy pełni dyżur. Nie powinien wprowadzać żadnych niestandardowych zmian w infrastrukturze tylko dlatego, że ma na to ochotę. Co więcej, nie wiemy, czy host bastionu został skonfigurowany w sposób zgodny, czy jest załatany, czy zarejestrowany w narzędziu do zarządzania zasobami, czy ma środki bezpieczeństwa i tak dalej. Działa jak nieudokumentowane tylne drzwi do środowiska, a jeśli zostanie wykorzystany, stanowi ogromne zagrożenie dla bezpieczeństwa. Bez względu na to, jak pracowity może być Alex, jego konfiguracja podważa szerszą politykę i praktyki. Jeśli Alex uważa, że usprawnienie procesu zdalnego dostępu przyniosłoby korzyści całej infrastrukturze, to powinien upewnić się, że pomysł na bastion hosta został zatwierdzony przez biznes jako autoryzowana metoda dostępu, o czym dowiesz się więcej, omawiając czwarte przykazanie. Wreszcie, praca w nieudokumentowany sposób utrudnia konserwację i rozwiązywanie problemów z systemami i usługami. Jest to pogwałcenie siódmego przykazania (przestrzegaj procedur). Alex powinien korzystać z dostarczonych narzędzi, a jeśli zadanie odbiega od znanego stanu, powinno być rejestrowane i dokumentowane. Na przykład, jeśli host bastionu Alexa zostanie naruszony, inne osoby mogą nie być świadome jego istnienia, nie podejrzewać jego roli w potencjalnej awarii lub nie mieć do niego dostępu. Co więcej, mogą nie wiedzieć, co robić, ponieważ mogło to zostać skonfigurowane w nietypowy sposób, który rozumie tylko właściciel.

Najlepsze procesy i narzędzia wspierające kulturę etyki

Do tej pory przyglądaliśmy się scenariuszowi z dwóch różnych punktów widzenia - konwersacji w toku oraz kilku wskazówek i wyjaśnień, w jaki sposób można go ulepszyć. Przeanalizowaliśmy to w odniesieniu do naszego pierwszego przykazania (Oddzielne role). Załóżmy teraz, że budujemy infrastrukturę IT od podstaw i mamy luksus nieograniczonego czasu i budżetu oraz żadnych duchów przeszłości centrów danych. Nie jesteśmy obciążeni przestarzałymi decyzjami, wymaganiami klientów lub przestarzałymi systemami, których nie można łatwo zmienić lub zaktualizować. Musi istnieć zdefiniowany proces zarządzania kontem. Ten proces musi być udokumentowany. Zasady, procedury i narzędzia wymienione w dokumentacji wymagają okresowego przeglądu. Należy wyraźnie oddzielić uprzywilejowaną pracę administracyjną od codziennej pracy, nawet z osobami, dla których administracja jest ich codzienną pracą. Nie wszystkie polecenia i akcje wymagają podwyższonych uprawnień i z reguły praca powinna być wykonywana na zwykłym koncie, dopóki nie będzie to już możliwe. Używanie konta uprzywilejowanego do prostych rzeczy, takich jak przeglądanie wiadomości e-mail lub otwieranie pliku, skazi konto, wypełniając plik dziennika bałaganem lub, w najgorszym przypadku, wprowadzając na konto złośliwe oprogramowanie. Powinny istnieć co najmniej trzy poziomy uprawnień - odzwierciedlone w trzech oddzielnych tożsamościach: konto osobiste, uprzywilejowane konto użytkownika i uprzywilejowane konto współdzielone. Istnieje również bardzo ważny rodzaj uprzywilejowanego konta współdzielonego: konto administracyjne. Powinny one w przejrzysty sposób mapować do różnych usług katalogowych. Zmiany w backendzie nie powinny zakłócać sposobu, w jaki użytkownik loguje się do systemów.

• Konto osobiste - unikalnie skojarzone z osobą, jest interfejsem pracownika do wykonywania swojej pracy. Praca wykonywana w ramach konta osobistego może mieć wpływ tylko na dane osoby. Na przykład nie możesz wprowadzać zmian w uprawnieniach lub własności cudzych plików. Konta osobistego nie należy używać do żadnej pracy, która może mieć wpływ na dane należące do innych osób lub funkcji w organizacji biznesowej.

• Konto użytkownika uprzywilejowanego - również powiązane z osobą, konto to jest interfejsem pracownika do wykonywania prac wymagających podwyższonych uprawnień. Na przykład pracownik może wykorzystać swoje uprzywilejowane konto do aktualizacji rekordu bazy danych lub uzyskać dostęp do niektórych danych w środowisku IT, które nie są dostępne dla wszystkich. Konto uprzywilejowanego użytkownika ucieleśnia zasadę konieczności poznania. Konta uprzywilejowanego użytkownika nie należy używać do jakiejkolwiek pracy osobistej; jeśli można go uzupełnić za pomocą konta osobistego, należy go najpierw użyć. To jest koncepcja najmniejszego przywileju.

• Uprzywilejowane konto współdzielone - nie jest jednoznacznie powiązane z daną osobą. Zamiast tego jest to zasób, który należy do zespołów, grup, funkcji biznesowych i usług. Na przykład serwer aplikacji może działać z określonym użytkownikiem ogólnym, a pracownicy z odpowiednimi poświadczeniami będą mogli przełączyć tożsamość na to uprzywilejowane konto współdzielone w celu administrowania usługą aplikacji. Bez dodatkowych środków (takich jak rejestrowanie i inspekcja) nie można prześledzić korzystania z uprzywilejowanego konta współdzielonego z osobami fizycznymi. Uprzywilejowane konto współdzielone powinno być używane do prac, których nie można wykonać za pomocą osobistego lub uprzywilejowanego konta użytkownika. Nie należy jej używać do jakiejkolwiek pracy związanej z indywidualnymi użytkownikami.

• Konto administracyjne - Specjalnym typem uprzywilejowanego konta współdzielonego jest konto administracyjne. Różni się tym, że jest używany specjalnie do zarządzania (krytycznymi) zasobami środowiska, które wymagają najwyższego poziomu uprawnień. W związku z tym niewłaściwe użycie konta administracyjnego może mieć znaczący wpływ na środowisko IT. Powinna być używana tylko do prac o najwyższym priorytecie, nagłych wypadków i prac, których nie można wykonać w inny sposób. Nie powinno to być wygodą ani skrótem do biurokratycznych przeszkód.

Wszystkie typy kont muszą być zarządzane w spójny sposób za pomocą pewnego rodzaju narzędzia do zarządzania uprawnieniami (takiego jak portal internetowy), zgodnie z zestawem zasad zarządzania uprawnieniami. Ogólnie uprawnienia powinny opierać się na kilku warunkach:

• Przywileje przyznawane tylko po pomyślnym zakończeniu weryfikowalnego procesu (takiego jak egzamin lub certyfikacja).

• Przywileje są tymczasowe - muszą wygasnąć po pewnym okresie (np. 90 dni).

• Przywileje muszą zostać zatwierdzone - Po wygaśnięciu; musi nastąpić proces odnowienia. Może być identyczny z początkowym procesem nadawania uprawnień lub nieco zmodyfikowany.

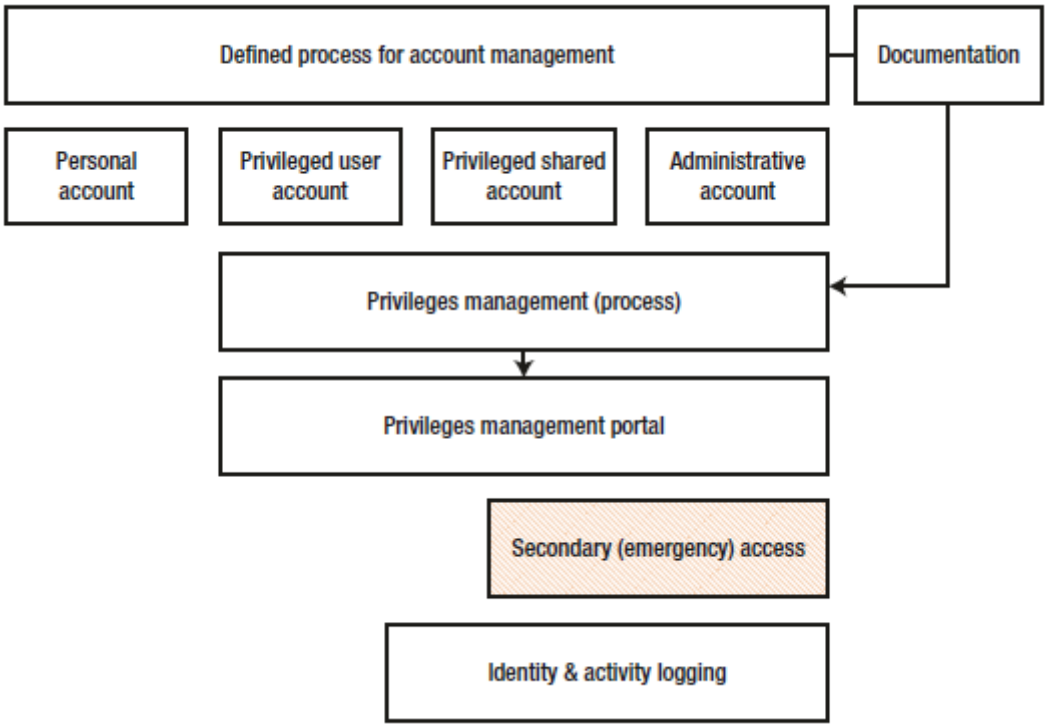
• Uprawnienia są szczegółowe - powiązane z określoną pracą, danymi lub systemami.

• Przydział uprawnień musi być udokumentowany - Proces dokumentacji może być ręczny, bazy danych lub bazy danych z wersjonowaniem (przechowywana jest cała historia).

• Wszystkie zmiany w przydzielonych uprawnieniach muszą być udokumentowane.

Uprzywilejowani użytkownicy (jeśli otrzymali pozwolenie, jak wspomniano wcześniej) muszą mieć możliwość żądania dostępu administracyjnego w jednolity sposób, który nie opiera się na żadnych ręcznych metodach, notatkach, ustnych wiadomościach lub podobnych. Portal intranetowy, o którym

Alex wspomniał Wendellowi, brzmi jak rozsądne rozwiązanie - użytkownicy identyfikują się z portalem, a następnie mogą otrzymać hasło administracyjne do natychmiastowego użycia. Jednak musi istnieć również dodatkowa metoda tworzenia kopii zapasowej, która umożliwia administratorom systemu uzyskanie uprzywilejowanego dostępu nawet w przypadku awarii systemów intranetowych. W ten sposób mogą uniknąć sytuacji impasu, w której potrzebują dostępu administracyjnego, ale nie mogą go uzyskać, ponieważ portal zarządzający hasłem jest niedostępny. W przypadku uprzywilejowanych kont współdzielonych i kont administracyjnych powinien istnieć mechanizm rejestrowania tożsamości, który może mapować sesję administracyjną i wszystkie wykonywane polecenia na odpowiedniego użytkownika. Na przykład można to zrobić za pomocą narzędzia opakowującego, które uruchamia sesję administracyjną i równolegle zapisuje dziennik poleceń. Wszystko to jest zmapowane na rysunku



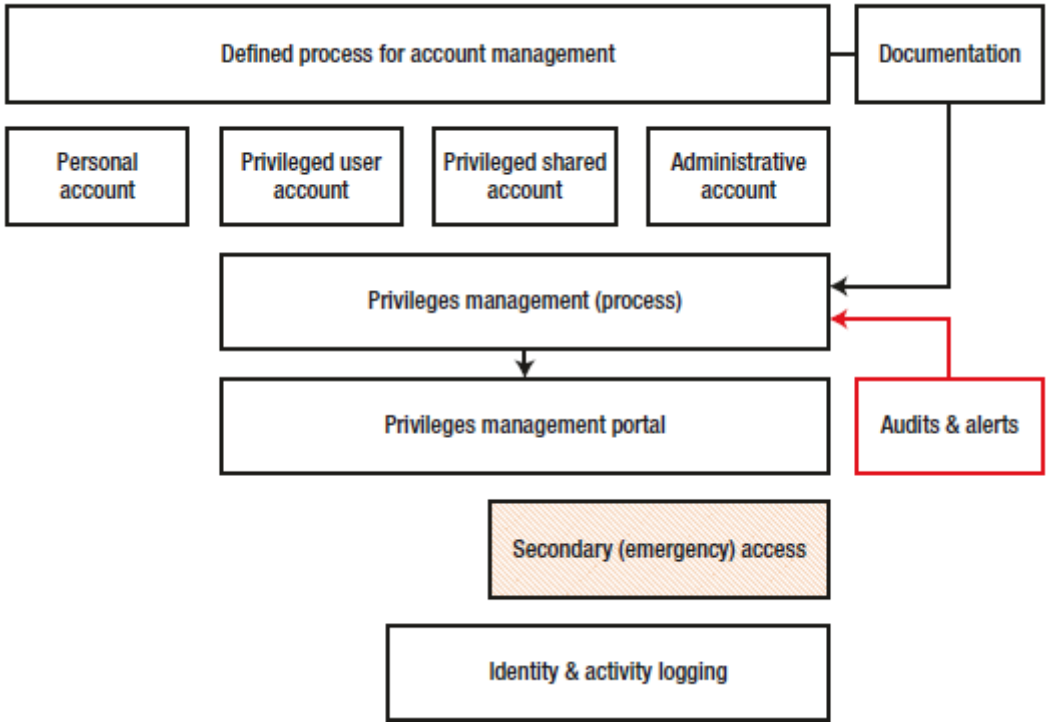
Rejestrowanie tożsamości i aktywności jest bardzo ważnym aspektem korzystania z konta uprzywilejowanego, a jego konstrukcja może mieć złożone efekty. Z jednej strony im więcej narzędzi jest wdrożonych, tym większa widoczność potencjalnych problemów i problemów, a także dowodów kryminalistycznych po przestojach, naruszeniach lub innych błędach związanych z pracą. Z drugiej strony, im więcej mechanizmów bezpieczeństwa znajduje się wokół systemów, tym bardziej rozpowszechnione staje się pojęcie Wielkiego Brata, maksyma skonceptualizowana w powieści George'a Orwella 1984. Wszyscy jesteśmy do niej podświadomie dostrojeni, a zwiększone bezpieczeństwo kojarzymy z nieufnością i podejrzliwością . Ktoś mógłby zapytać: „Dlaczego firma musi pilnować tego, co robią pracownicy, czy nie ma zaufania?" Rzeczywiście, silne zabezpieczenie może zniechęcać do przypadkowych przestępstw, ale stwarza też poczucie, że każdy jest traktowany jako potencjalny przestępca, co może wywoływać negatywne emocje w miejscu pracy. Może nawet zachęcić ludzi do obchodzenia mechanizmów bezpieczeństwa, zwłaszcza jeśli przeszkadzają w pracy. Jak na ironię, dość często usługi rejestrowania tożsamości były wprowadzane do środowisk IT w wyniku niezbyt starannego korzystania z uprzywilejowanych kont i narzędzi, tworząc chaos i szkody przy niewielkich lub zerowych dowodach kryminalistycznych wyjaśniających, dlaczego i w jaki sposób wystąpiły problemy. W ten sposób staje się cyklem samozasilania: jeśli pracownicy przyjmą systemy i mechanizmy bezpieczeństwa (i przezwyciężą ideę nieufności), tym mniej istotne stają się wdrażane

środki. Podobnie, im więcej „podziemnej” pracy jest wykonywanych, tym bardziej kierownictwo firmy może odczuwać potrzebę wprowadzenia narzędzi zapewniających przejrzystość i strukturę do codziennej administracji. Musi istnieć zdrowa równowaga między pracą uprzywilejowaną, rejestrowaniem tożsamości i zaufaniem do pracowników. W tym miejscu w grę wchodzą koncepcje audytów, alertów i automatyzacji, ponieważ mogą one pomóc nam w budowaniu solidnej infrastruktury opartej na zaufaniu, a także dobrych ścieżkach danych.

Audyty i alerty

Musimy mieć pewność, że stosowane przez nas narzędzia i kontrole pozostają ważne i aktualne oraz że jesteśmy w stanie szybko wykryć i naprawić wszelkie odstępstwa od pożądanego stanu bezpiecznego i zgodnego z przepisami. Jeśli potraktujesz każdy warunek, który zapisaliśmy wcześniej, jako scenariusz „jeśli-to”, wówczas będzie to potencjalny punkt awarii w systemie. Na przykład, jeśli hasło do konta uprzywilejowanego wymaga rotacji co 90 dni, w tym scenariuszu należy skonfigurować alert, aby zachować zgodność.

Nasza infrastruktura zarządzania kontami będzie kompletna i w pełni skuteczna tylko wtedy, gdy będziemy mieć również audyty i alerty, które mogą nas ostrzec, że nie spełniono niektórych wymaganych warunków na dowolnym skrzyżowaniu drzewa decyzyjnego.



Innymi słowy, na każde pojedyncze wymaganie, które stworzyliśmy, potrzebujemy również

• Wynik wymierny

• Walidacja oparta na czasie

• Zapis wykonanych działań (archiwum i audyt)

• Powiadomienie o pominiętym działaniu lub wyniku negatywnym/fałszywym

Jeśli użytkownikowi przyznano podwyższone uprawnienia, należy to sprawdzić. Jeżeli takie uprawnienia zostały przyznane bez sprawdzenia niezbędnych kryteriów eksperckich, system

monitorowania powiadomi. Jeśli konto naruszy którykolwiek z podanych warunków, system monitorowania powiadomi. Pozwala to na pełną świadomość sytuacyjną i sprężyste środowisko, które niepostrzeżenie nie odbiega od zamierzonego stanu (jak to często bywa w biznesach IT).

Automatyzacja

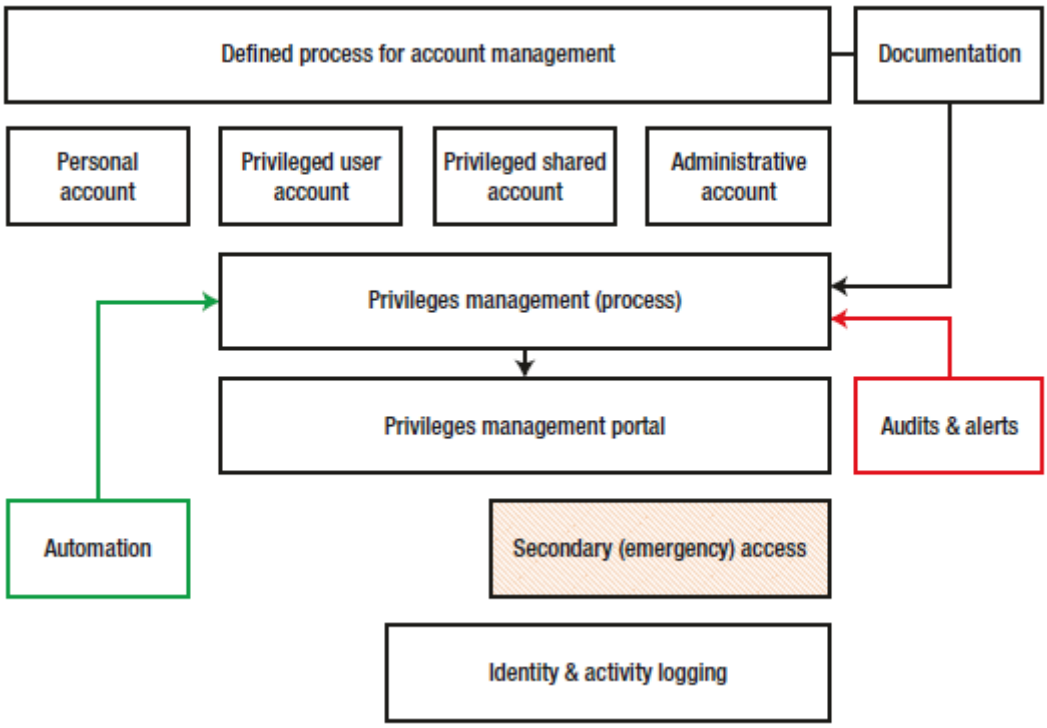
Wciąż możemy zrobić więcej. Automatyzacja jest ważnym elementem skutecznego zarządzania systemami. Automatyzacja zmniejsza obciążenie pracą, minimalizuje błędy i pozwala lepiej śledzić wykonaną pracę. Należy go używać zawsze, gdy wymagana jest powtarzalna praca – niezależnie od tego, czy jest to to samo polecenie wykonywane wielokrotnie, czy to samo polecenie uruchamiane na wielu hostach. Jeśli możesz zdefiniować proces pracy w procesie deterministycznym – jasny zestaw warunków „jeśli-to" z wymiernymi wynikami – możesz zautomatyzować takie procesy. Istnieje kilka przykładów automatyzacji, które można zastosować, szczególnie do zarządzania kontami:

• Tworzenie konta użytkownika jest w pełni skryptowe – po podaniu podstawowych informacji środowisko użytkownika jest automatycznie konfigurowane: limity danych, uprawnienia, foldery osobiste i służbowe itp. W wysoce zautomatyzowanym środowisku aktywowany jest akt zatwierdzenia konta utworzenie konta. Narzędzia do zarządzania tożsamością i dostępem, takie jak SailPoint4, można skonfigurować tak, aby zapewniały pełną automatyzację na wielu kontach.

• Zarządzanie hasłami użytkowników – przeprowadzane są różne kontrole w celu zapewnienia, że hasła są zarządzane prawidłowo i zgodnie z polityką firmy.

• Zarządzanie środowiskiem – narzędzia sprawdzające każdy system w środowisku pod kątem niestandardowych kont lub folderów, niewystarczających uprawnień, nieodpowiednich środków bezpieczeństwa i nie tylko. Taka praktyka może zmniejszyć obciążenie administratorów systemów i pozwolić na skupienie się na kwestiach etycznych, gdy się one pojawią.

Najczęstszym sposobem automatyzacji administrowania systemem jest użycie narzędzi do zarządzania konfiguracją (CM). Koncepcja narodziła się w latach pięćdziesiątych XX wieku, aby ułatwić zarządzanie zapasami, ale w branży IT staje się niezbędna. Deterministyczny charakter oprogramowania oraz względna jednorodność systemów i usług pozwalają na efektywne wykorzystanie narzędzi, które mogą masowo wdrażać lub konfigurować środowisko. Zazwyczaj będzie serwer CM, który przechowuje szablony konfiguracji dla różnych usług lub systemów. Klienci (hosty lub aplikacje) będą kontaktować się z serwerem z określoną częstotliwością odpytywania i pobierać te konfiguracje. Zapewnia to ujednolicenie i ręczne zmiany są usuwane. Ułatwia to również przeprowadzanie audytów i ostrzeganie. Obok CM dostępne są także narzędzia do wersjonowania, które pomagają stworzyć historię wykonanej pracy, niezależnie od tego, czy są to polecenia, czy zmiany w szablonach pracy (tzw. zatwierdzenia). Istnieje ogromna różnorodność oprogramowania CM. Do najpopularniejszych należą CFEngine,5 Chef,6 Puppet,7 i Ansible8, w związku z czym ich szablony konfiguracyjne nazywane są przepisami lub podręcznikami. Obecnie CM ewoluował, obejmując różne metodologie branżowe w celu zwiększenia szybkości cyklu życia zarządzania oprogramowaniem. Czasami służy również do ułatwienia tworzenia oprogramowania i administrowania systemem, lepiej znanym pod popularnym terminem DevOps. Automatyzacja nie musi jednak opierać się na drogich i skomplikowanych narzędziach. Nie pozwól, aby ograniczenia operacyjne lub wymagania związane z korzystaniem z kompleksowego oprogramowania do zarządzania konfiguracją i wersjonowania Cię zniechęciły. Możesz stworzyć własną automatyzację. Możesz użyć skryptów BASH lub PowerShell, aby zautomatyzować tworzenie kont użytkowników lub inspekcję. Zaplanowanych zadań można używać do okresowego sprawdzania niezgodności. Możesz użyć lokalnego serwera pocztowego, aby wysłać powiadomienia do administratorów systemu, jeśli znajdziesz rozbieżności w procesach lub bezpieczeństwie. Każdy najmniejszy wysiłek pomaga zapewnić przejrzystość i jakość pracy. Pokazano to bardziej szczegółowo na rysunku.



Znaczenie tych środków polega na tym, że wprowadzają one strukturę do praktyk pracy i redukują hałas operacyjny. To z kolei może pomóc administratorom systemu postępować bardziej etycznie – nie musisz się martwić ręcznym wprowadzaniem zmian na kontach użytkowników (co może powodować błędy i obciążenie oraz „zachęcać" ludzi do pójścia na skróty), skupiasz się na zapewnieniu solidnego i zautomatyzowanego infrastrukturę zbudowaną w oparciu o solidne zasady etyczne.

Dlaczego to wszystko jest takie ważne?

Podstawowym problemem w przypadku etyki kontra technologii jest to, że jest to jedna wielka szara strefa. Sprawy rzadko są czarno-białe. Z drugiej strony oprogramowanie jest deterministyczne, a ludzie szukają deterministycznych rozwiązań problemów technologicznych. Oznacza to, że firmy zainwestują wiele wysiłku i pieniędzy w tworzenie doskonałych rozwiązań z punktu widzenia technologii, ale zapominają lub ignorują ludzkie równanie. Niestety, ludzkiej strony rzeczy nie da się rozwiązać za pomocą oprogramowania.

Nie przejdziesz

Z czasem uzyskanie uprzywilejowanego dostępu stało się bardziej złożone. Wiemy, że popełniamy błędy, dlatego staramy się, aby popełnianie błędów było trudniejsze – ale nie niemożliwe. Czasami zakładamy, że błędy będą nieuniknione (podejście Design for Failure [DFF]), więc nie jest to kwestia, czy; staje się grą o to, kiedy i ile – minimalizując szkody i będąc w stanie wcześnie zatrzymać błędy i szybko reagować. Staramy się także na bieżąco śledzić naszą pracę, aby mieć wystarczającą ilość danych, aby omówić awarie i problemy po fakcie. Zakłada się również, że ludzie będą mniej podatni na robienie „złych" rzeczy, jeśli wiedzą, że zostaną złapani – to etyka wkradająca się do świata technologii. Aby w pełni zrozumieć znaczenie etyki kontra technologii, porozmawiajmy trochę o szkodach.

Uszkodzenie jako usługa

Problemy związane z pracą objawiają się w następujący sposób:

• Przypadek 1: Zła ocena – ludzie podejmują złą decyzję.

• Przypadek 2: Niewystarczające informacje – ludzie działają w oparciu o ograniczony zestaw dostępnych danych.

• Przypadek 3: Brak procedur i umiejętności – Ludzie powodują szkody w wyniku połączenia źle zdefiniowanych procedur pracy i niewystarczającej wiedzy w temacie.

• Przypadek 4: Celowy sabotaż.

Przypadku 1 nie można naprawić za pomocą oprogramowania – można go jedynie złagodzić. Czasami ludzie będą nawet obchodzić istniejące mechanizmy bezpieczeństwa, aby wykonać swoją pracę, mając pełne przekonanie, że to, co robią, jest słuszne. Filtry programowe można wykorzystać do zatrzymania niektórych oczywistych błędów (takich jak usunięcie całej bazy danych lub sformatowanie dysku twardego) lub do spowolnienia wykonywania błędnych poleceń (celowe opóźnienie w przypadku zadań wsadowych uruchamianych na wielu hostach). Przestrzeganie ścisłego podziału ról i używanie najmniejszych uprawnień potrzebnych do wykonania zadania może pomóc zminimalizować szkody. Monitorowanie i alerty to podstawa każdego administratora systemu, szczególnie w środowisku o dużej skali – dobrze zaprojektowane rozwiązanie gwarantuje, że reagujesz tylko na najważniejsze i istotne problemy, a nie na fałszywe błędy lub fałszywe alarmy. Alerty monitorowania rzadko mają charakter poufny, ale czasami oprócz alertów wymagane są dodatkowe informacje na temat kontekstu i metadanych, aby umożliwić dalsze rozwiązywanie problemów. Te dodatkowe informacje mogą być poufne. W mojej firmie jedna z osób zajmujących się wsparciem zdecydowała się na przesyłanie alertów na swój osobisty identyfikator e-mail, aby można było uzyskać do nich dostęp z dowolnego miejsca. Stało się tak pomimo określonej polityki zakazującej takiego postępowania. Działanie zostało wykryte podczas audytu bezpieczeństwa, a wobec osoby wszczęto postępowanie dyscyplinarne. Przypadek 2 jest jeszcze trudniejszy do naprawienia – ponieważ polegamy na ludziach podejmujących decyzje w oparciu o nieoptymalny zestaw danych. W rzeczywistości można nawet zachęcać do celowych „błędów", aby pomóc nauczyć się radzić sobie w nieznanym scenariuszu (masz serwer, na którym aktualnie działają przepływy klientów, ale ze względu na obciążenie serwera nie możesz się zalogować i sprawdzić dlaczego). Należy pamiętać: im więcej masz przywilejów, tym bardziej musisz zachować ostrożność. Jeśli nie masz pewności co do potencjalnych konsekwencji działania, nie powinieneś używać konta uprzywilejowanego do testowania wyniku. Przypadkowi 3 można zapobiec – pod warunkiem, że infrastruktura IT posiada solidne mechanizmy, które dopasowują umiejętności i wiedzę do przywilejów. Należy jednak pamiętać, że często występuje silny element miękki – nauczanie, coaching, mentoring, zajęcia, egzaminy i wreszcie podejmowanie decyzji, aby umożliwić komuś dostęp do uprzywilejowanych zasobów, jeśli wykaże się wystarczającym poziomem wiedzy specjalistycznej. Przyjrzymy się temu bardziej szczegółowo, gdy będziemy omawiać inne przykazania. Historycznie rzecz biorąc, większość koncepcji rozdziału obowiązków i przywilejów wywodzi się z tego przypadku (a nie z przypadku 1, jak można by przypuszczać). Jeśli oglądałeś wiadomości w 2013 roku, bez wątpienia widziałeś doniesienia o włamaniach i kradzieży danych kont płatniczych klientów z kilku dużych firm, w tym giganta handlu detalicznego Target. Hakerzy wykorzystali wiele metod, aby przedostać się przez różne zapory ogniowe i systemy, aby umieścić na komputerach złośliwe oprogramowanie w celu gromadzenia prywatnych danych klientów. Możemy jedynie spekulować, jakie zwroty akcji wykorzystali hakerzy w celu znalezienia, zebrania, a następnie odzyskania wrażliwych danych; wiemy jednak z „aktualizacji zabezpieczeń i ulepszeń technologii Target" firmy Target, jakie kroki podjęła firma Target, aby zapobiec podobnym naruszeniom w przyszłości. Ulepszenie monitorowania i rejestrowania, instalacja systemów punktów sprzedaży z białą listą aplikacji, wdrożenie ulepszonej segmentacji, przeglądanie i ograniczanie dostępu dostawców oraz zwiększone bezpieczeństwo kont to pięć głównych obszarów ulepszeń. Rozdzielenie ról poprzez zwiększone bezpieczeństwo kont było główną częścią ich planu działania. Ograniczając dostęp dostawców, zmniejszając uprawnienia kont,

wyłączając konta dostawców i rozszerzając magazyny haseł, wyeliminowali wiele możliwych do wykorzystania uprzywilejowanych celów w swoim środowisku komputerowym. Rozszerzając zastosowanie uwierzytelniania dwuskładnikowego i opracowując dodatkowe szkolenia z zakresu stosowania rotacji haseł, upewnili się, że osoby korzystające z kont są właściwymi użytkownikami. Ulepszony monitoring pozwoliłby wykryć wiele exploitów, zwłaszcza gdyby wdrożono automatyzację i procesy umożliwiające szybkie reagowanie na alerty. Jestem pewien, że dostawcy pracujący w tych dużych firmach nalegają obecnie na te zabezpieczenia, aby nie zostać oskarżonymi o kolejny exploit komputerowy. Przypadek 4 jest najtrudniejszy. Nie ma technologii, która powstrzyma zdeterminowaną złośliwość, szczególnie w obrębie firmy. Pracownik mający dostęp do uprzywilejowanych zasobów będzie w stanie, mając wystarczająco dużo czasu i wystarczających możliwości, ominąć nawet najbardziej skomplikowane rozwiązania. Niestety, zbyt wiele wysiłku marnuje się na ochronę firm przed tym (narożnym) przypadkiem, zamiast skupiać się na pierwszych trzech przypadkach. Stwarza to również złożony problem – im większy brak zaufania „zainwestujesz" w swój stos technologiczny, tym bardziej kruche staje się ludzkie równanie. Będzie odzwierciedlać podejmowanie ryzyka, innowacyjność, szybkość zmian, koszty i morale. Ale skomplikujmy sprawę jeszcze bardziej, dobrze?

Kompas Wskazuje Południe

Najważniejszym problemem nie jest „samotny wariat", który sieje spustoszenie w zasobach IT firmy. Jest to niewidzialne przechodzenie „dobrych ludzi" w kierunku nieetycznych działań, którego nikt tak naprawdę nie zauważa. W rozmowie Alexa i Wendella nowy pracownik od samego początku był narażony na nieetyczne zachowanie. Alex działał z pozycji autorytetu (zakładając słuszność) i – co najgorsze – mógł nawet nie być świadomy, że robi coś złego! Przez lata Alex wypracował praktyki, które najlepiej odpowiadały jego stylowi i potrzebom. Stworzył hosta bastionu, aby ułatwić mu pracę (na pozór to dobrze, ponieważ Alex może zrobić więcej dla biznesu). To samo podejście doprowadziło go do zapewnienia Belindzie uprzywilejowanego dostępu. Kompas moralny Alexa działa dobrze – jeśli chodzi o Alexa. Może też nie być w stanie uzewnętrznić swoich działań i spojrzeć na nie z obiektywnej perspektywy. Jest to przypadek pełzania błędów poznawczych. Rosnące uprzedzenia objawiają się na wiele sposobów – ignorujemy niepowodzenia, ufamy informacjom, które potwierdzają nasze przekonania i uprzedzenia, ignorujemy te, które są z nimi sprzeczne lub zaprzeczają, a ponieważ wydaje się, że coś, co robimy, działa, rób to dalej. Dotyczy to nas wszystkich; często robimy coś z przekonaniem, że postępujemy w najlepszy (i najbardziej etyczny) sposób. Po drodze popełniamy błędy, ponieważ nigdy nie mieliśmy złotego punktu odniesienia, według którego moglibyśmy mierzyć nasze działania.

Wniosek

Zarządzanie kontem jest jedną z najważniejszych rzeczy w systemie administracji, ponieważ ostatecznie wszystko sprowadza się do dostępu i uprawnień użytkowników oraz tego, co ludzie mogą zrobić, mając odpowiednie uprawnienia. Jest to również pole do popisu dla naruszeń zasad etycznych, zarówno zamierzonych, jak i niezamierzonych. Możemy chronić się jedynie przed ograniczoną liczbą scenariuszy, w których szkody powstają w sposób umyślny. Zamiast tego musimy skupić się na dużej i złożonej szarej strefie, w której nieetyczne zachowanie ma miejsce w wyniku pominięcia procedur, źle zdefiniowanych kroków, sprzecznych instrukcji i osobistych nawyków. Najlepszym sposobem, aby administratorzy systemów zabezpieczyli się przed sobą i zminimalizowali ryzyko szkód w środowisku IT, jest rozdzielenie ról. Z kont uprzywilejowanych należy korzystać tylko wtedy, gdy jest to absolutnie konieczne. Każde takie użycie powinno być rejestrowane, aby możliwe było łatwe i przejrzyste debugowanie wszelkich problemów. Kont uprzywilejowanych nie można używać do celów osobistych, nawet jeśli pozornie pomagają one w pracy. Zdrowe środowisko IT będzie wyposażone w monitory, które będą w stanie wykrywać i ostrzegać o wszelkich naruszeniach technicznych w procesie

zarządzania kontem, aby można było je szybko naprawić. Teraz, gdy mamy uprzywilejowany dostęp, jesteśmy narażeni na zupełnie nowy zakres wyzwań, z których najważniejszym jest prywatność.