PRAKTYKI I POLITYKI ZATRUDNIENIA

WPROWADZANIE

Przestępczość to kwestia ludzka, a nie tylko technologiczna. To prawda, że technologia może zmniejszyć częstość występowania przestępstw komputerowych, ale podstawowym problemem jest to, że ludzie mogą ulec pokusie wykorzystania wad naszych systemów informatycznych. Najbardziej spektakularna biometryczna kontrola dostępu na świecie nie powstrzyma kogoś przed wejściem do pokoju komputerowego, jeśli woźny uzna, że to „tylko po to, by odebrać wizytówkę". Ludzie są kluczem do skutecznego bezpieczeństwa informacji, a niezadowoleni pracownicy i rozgniewani byli pracownicy są, według wielu aktualnych badań, poważnymi zagrożeniami. Tu przedstawiono zasady integracji zarządzania zasobami ludzkimi (HR) i bezpieczeństwem informacji z kulturą korporacyjną.

ZATRUDNIENIE

Jakość pracowników jest podstawą sukcesu wszystkich przedsiębiorstw; to także podstawa skutecznego bezpieczeństwa informacji.

Sprawdzanie pochodzenia kandydata.

Szczególnym problemem jest zatrudnianie nowych pracowników; coraz więcej dowodów sugeruje, że wiele osób zawyża swoje życiorysy bezpodstawnymi twierdzeniami. Według Edwarda Andlera, autora The Complete Reference Checking Handbook, „oszukiwanie życiorysów stało się niepokojąco powszechne. I wielu ludzi sobie z tym radzi, co wydaje się skłaniać innych do naśladowania. Jego badania pokazują, że nawet 10 procent „poważnie błędnie przedstawia" swoje pochodzenie lub historię pracy. Projekt badawczy prowadzony przez Port Authority of New York and New Jersey użył reklamy z prośbą o elektryków, którzy byli ekspertami w używaniu „złącz Sontag". Otrzymali 170 odpowiedzi twierdzących, że taka ekspertyza, mimo że takiego urządzenia nie było. Recenzenci powinni szczególnie uważać na niejasne słowa, takie jak „monitorowany" i „wtajemniczony". Podczas rozmów kwalifikacyjnych lub sprawdzania przeszłości pracownicy HR powinni w miarę możliwości szczegółowo dowiedzieć się, co zrobił kandydat. Należy sprawdzić wszystkie referencje, przynajmniej w celu sprawdzenia, czy kandydaci rzeczywiście pracowali tam, gdzie według życiorysu pracowali. Niestety, przy rozpatrywaniu czyjejś karalności pojawia się problem wolności obywatelskich. Gdy ludzie ponieśli prawnie przewidzianą karę za przestępstwo, czy to grzywny, prace społeczne lub pozbawienie wolności, dyskryminując ich w zatrudnianiu może stanowić naruszenie ich praw obywatelskich. Czy można wykluczyć skazanych przestępców z jakichkolwiek ofert pracy? Z wakatów podobnych do obszarów, w których nadużyli zaufania dawnych pracodawców? Czy pracodawcy mogą zgodnie z prawem wymagać, aby potencjalni pracownicy zatwierdzali weryfikację przeszłości? Czy można prawnie wymagać badań wariografem? Testy narkotykowe? Testy osobowości? W niektórych jurysdykcjach „niedbałe zatrudnienie", które powoduje szkody dla osób trzecich, jest karane w postępowaniu cywilnym. Wyobraź sobie na przykład, że firma miałaby zatrudnić aktywnego hakera-kryminalistę jako administratora systemu bez odpowiedniego sprawdzania przeszłości i rozmów kwalifikacyjnych; gdyby haker wykorzystał swoją pozycję i zasoby korporacyjne do włamania się lub sabotowania systemów innej organizacji, uzasadnione jest przypuszczenie, że ofiara mogłaby domagać się odszkodowania od pracodawcy przestępcy z powodu zaniedbania w zatrudnieniu. Ponadto „niedbałe zatrzymanie" może pociągnąć pracodawcę do odpowiedzialności, gdy pracownik, który może stanowić zagrożenie dla współpracowników lub społeczeństwa, nie zostanie zwolniony z pracy od razu. Pracodawcy powinni konsultować się z personelem prawnym korporacji, aby upewnić się, że znają swoje prawa i obowiązki oraz stosują je w konkretnym kontekście prawnym ich pracy. Nawet sprawdzanie referencji od poprzednich pracodawców jest obarczone niepewnością. Pracodawcy mogą wahać się przed wystawieniem złych referencji niekompetentnym lub nieetycznym pracownikom z

obawy przed procesami sądowymi, jeśli ich komentarze zostaną ujawnione lub jeśli pracownik nie otrzyma nowej pracy. Dziś nie można liczyć na odpowiedź na proste pytanie „Czy zatrudniłbyś ponownie tego pracownika?" Byli pracodawcy muszą również uważać, aby nie zawyżać swojej oceny byłego pracownika. Ogromne pochwały dla łajdaka mogą doprowadzić do pozwu ze strony niezadowolonego nowego pracodawcy. Z tych powodów coraz większa liczba pracodawców stosuje zasady korporacyjne, które zabraniają omawiania wyników byłego pracownika w jakikolwiek sposób, pozytywny lub negatywny. Wszystko, co otrzymuje się od kontaktu w takich przypadkach, to „Twój kandydat pracował jako inżynier klasy 3 w latach 1991-1992. Nie wolno mi podawać żadnych dalszych informacji". W dziedzinie bezpieczeństwa powszechne jest, że niektóre osoby, które skutecznie popełniły przestępstwa, były nagradzane „złotym uściskiem dłoni" (specjalna zapłata w zamian za odejście), czasem nawet pozytywnymi referencjami. Przestępcy mogą następnie przejść do wiktymizacji nowego pracodawcy. Nikt jednak nie wie, jak często to się dzieje. Aby obejść takie zniekształcenia, ankieterzy powinni uważnie wypytać kandydatów o szczegóły ich wykształcenia i doświadczenia zawodowego. Odpowiedzi można następnie sprawdzić pod kątem spójności wewnętrznej i porównać z pisemnymi oświadczeniami kandydata. Kłamcy nienawidzą szczegółów: o wiele trudniej jest zapamiętać, które kłamstwo powtórzyć komu, niż powiedzieć prawdę. Istnieją usługi komercyjne specjalizujące się w sprawdzaniu przeszłości (np. Achievement Tec). Zapewniają one niezbędne formularze, aby umożliwić pracodawcom sprawdzanie zapisów kredytowych i innych informacji ogólnych. Firmy takie jak Kroll i Securitas Security Services również przeprowadzają szeroko zakrojone kontrole przeszłości. Innym sposobem sprawdzenia pracowników może być bezpłatne lub niewielkie za pośrednictwem wyszukiwarek internetowych. Wpisując czyjeś nazwisko do jednej z tych wyszukiwarek, istnieje duże prawdopodobieństwo, że zostanie odzyskany jakiś aspekt życia wnioskodawcy. Szczególnie interesujące może być wyszukiwanie wiadomości z konkretnego bloga, aby zobaczyć, jakie informacje są rozpowszechniane. Doświadczeni pracownicy powinni przeprowadzić rozmowę kwalifikacyjną z kandydatem i porównać notatki na spotkaniach, aby wykryć niespójności. Dyrektor pomocy technicznej w dużym biurze obsługi komputerów przesłuchał nowego pracownika, który twierdził, że pracował na danej platformie od kilku lat, ale nie wiedział, jak się zalogować. Gdyby przed zatrudnieniem porozmawiał z którymkolwiek z programistów, jego oszustwo zostałoby szybko odkryte. Jak na ironię, gdyby powiedział prawdę, i tak mógłby zostać zatrudniony.

Umowy o pracę

Przed dopuszczeniem nowych pracowników do podjęcia pracy, powinni oni podpisać umowę o pracę, która stanowi, że nie będą ujawniać informacji poufnych ani tajemnic handlowych swoich poprzednich pracodawców. Kolejna klauzula musi stwierdzać, że rozumieją, że nowy pracodawca wyraźnie nie żąda dostępu do informacji przywłaszczonych od poprzedniego pracodawcy lub z jakiegokolwiek innego źródła. Jednolita ustawa o tajemnicach handlowych, która jest egzekwowana w wielu jurysdykcjach w Stanach Zjednoczonych, przewiduje kary do trzykrotności wykazanych szkód finansowych, plus honoraria adwokackie spowodowane takim wyciekiem danych. Jedna głośna sprawa dotyczyła trzech pracowników, których uznano winnymi kradzieży i próby sprzedania sekretów Coca-Coli konkurencyjnej firmie Pepsi.

ZARZĄDZANIE

Bezpieczeństwo jest wynikiem kultury korporacyjnej; dlatego praktyki zarządzania są niezwykle ważne dla skutecznej ochrony informacji. Ataki zewnętrzne za pośrednictwem połączeń internetowych i uszkodzenia powodowane przez złośliwe oprogramowanie są z pewnością ważnymi zagrożeniami; niemniej jednak szkody wewnętrzne spowodowane błędami i pominięciami, a także nieuczciwością lub chęcią zemsty są nadal głównymi problemami w zakresie bezpieczeństwa informacji.4 Problemy te

potęgują się, gdy istnieją zagrożenia związane ze współpracą z udziałem osób poufnych pracujących z osobami spoza przedsiębiorstwa.

Zidentyfikuj możliwości nadużyć

Menedżerowie ds. bezpieczeństwa nie muszą popadać w paranoję, po prostu muszą zachowywać się tak, jakby byli paranoikami. Menedżerowie muszą traktować ludzi ze skrupulatną i uczciwą uwagą na pisemnych zasadach i procedurach. Wybiórcze lub kapryśne egzekwowanie procedur może stanowić nękanie. Jeśli niektóre osoby mogą przebywać same w drukarni podczas drukowania czeków płacowych, podczas gdy inni pracownicy równorzędnej rangi muszą być w towarzystwie, ci ostatni mogą zasadnie zinterpretować tę niezgodność jako dorozumianą oznakę nieufności. Takie traktowanie może skłaniać niektórych pracowników do wszczynania zażaleń i pozwów cywilnych, do składania skarg karnych o dyskryminację, a nawet do popełnienia zemsty.

Dostęp nie jest ani przywilejem, ani prawem

Gdy kierownictwo odbiera prawa dostępu do serwerowni sieciowej analitykowi systemu, który nie ma powodu, aby wchodzić w ten obszar, odpowiedzią mogą być urazy, dąsy i nadużycia. Ludzie czasami traktują kontrolę dostępu jako symbole statusu; z jakiego innego powodu dyrektor generalny, który nie ma przeszkolenia technicznego, żądałby, aby jego kod dostępu zawierał bibliotekę taśm i szafkę z okablowaniem? Menedżerowie mogą pokonać te psychologiczne bariery w celu zwiększenia bezpieczeństwa, wprowadzając inny sposób patrzenia na luki w zabezpieczeniach i dostęp. Po zidentyfikowaniu przez danego pracownika możliwości korzystania z systemu w sposób nieuprawniony, dyskusję należy zamienić w kwestię ochrony osoby, która ma niepotrzebny dostęp, przed nieuzasadnionymi podejrzeniami. Na przykład pracownik mający większy dostęp do zabezpieczonych plików niż jest to wymagane, jest narażony na ryzyko. Gdyby coś poszło nie tak z zabezpieczonymi plikami, ten pracownik byłby podejrzanym. Nie ma potrzeby formułować problemu w kategoriach podejrzliwości i nieufności. Mając na uwadze te zasady, menedżerowie powinni być wyczuleni na takie zagrożenia, jak umożliwienie pracownikowi samotności w wrażliwym obszarze, umożliwienie nienadzorowanego dostępu do niezaszyfrowanych kopii zapasowych lub posiadanie tylko jednego programisty, który wie cokolwiek o wewnętrznych elementach pakietu księgowego. Jeśli chodzi o język, lepiej byłoby przestać odwoływać się do przywilejów dostępu. Samo słowo kojarzy się z wyższością i statusem – ostatnie rzeczy, które zarządzanie powinno sugerować. Dostęp jest funkcją i obowiązkiem, a nie przywilejem czy prawem; należy je nazywać po prostu funkcjami dostępu lub uprawnieniami dostępu.

Niezbędny pracownik

W wielu obszarach przetwarzania informacji nadmiarowość jest ogólnie postrzegana albo jako coś złego, albo jako nieunikniony, ale godny pożałowania koszt zapłacony za określone korzyści. Na przykład w bazie danych indeksowanie może wymagać umieszczenia identycznych pól (elementów, kolumn) w osobnych plikach (zestawy danych, tabele) w celu ustanowienia połączeń (widoków, złączeń). Jednak w zarządzaniu personelem dla lepszego bezpieczeństwa wymagana jest redundancja. Bez wspólnej wiedzy organizacja jest stale narażona na naruszenie dostępności. Redundancja w tym kontekście oznacza posiadanie więcej niż jednej osoby, która może wykonać dane zadanie. Innym sposobem patrzenia na to jest to, że żadna wiedza nie powinna należeć tylko do jednej osoby w organizacji. Oddanie kluczy do królestwa w ręce jednego pracownika grozi katastrofą. Unikalne zasoby zawsze narażają systemy na ryzyko; dlatego firmy takie jak Tandem, Stratus i inne z takim powodzeniem dostarczają redundantne i odporne na błędy systemy komputerowe do zadań krytycznych, takich jak giełdy i sieci bankowe. Te systemy komputerowe i sieci mają dwa procesory, kanały, macierze pamięci, dyski i kontrolery. Podobnie organizacja odporna na błędy zainwestuje w

przeszkolenie wszystkich swoich pracowników. Każde zadanie powinno mieć co najmniej jedną inną osobę, która wie, jak to zrobić - nawet jeśli mniej dobrze niż podstawowy zasób. Zasada ta nie oznacza, że menedżerowie muszą tworzyć klony wszystkich swoich pracowników; w rzeczywistości lepiej jest mieć kilka osób, które mogą wykonywać różne części pracy jednej osoby. Rozpowszechnienie wiedzy w całej organizacji pozwala ograniczyć szkody spowodowane nieobecnością lub niedostępnością kluczowych osób. Niebezpieczne jest, aby jeden pracownik był jedyną osobą, która wie o krytycznej funkcji w przedsiębiorstwie. Operacje ucierpią, jeśli kluczowa osoba będzie nieobecna, a przedsiębiorstwo z pewnością ucierpi, jeśli ta unikalna osoba z zasobów zdecyduje się zachowywać w nieautoryzowany i szkodliwy sposób. Menedżerowie powinni zadać sobie pytanie, czy w ich dziale jest ktoś, kogo nieobecności obawiają się. Czy istnieją jakieś krytyczne, ale nieudokumentowane procedury, o które każdy musi poprosić konkretną osobę? Klient z klasy zarządzania operacjami centrum danych zgłosił na ochotnika następującą historię. Był kreator programowania odpowiedzialny za utrzymanie kluczowego programu produkcyjnego; niestety miał słabe umiejętności komunikacyjne i wolał sam rozwiązywać problemy niż trenować i angażować kolegów. „Szybciej zrobię to samemu", zwykł mawiać. Podczas jednego z jego rzadkich wakacji coś poszło nie tak z „jego" programem produkcyjnym, zamykając działalność firmy. Czarodziej przebywał w północnych lasach, poza zasięgiem wszelkiej komunikacji; katastrofa trwała, dopóki on… został zwrócony. Cierpi nie tylko organizacja, ale także niezastąpione osoby cierpią z powodu braku równowagi wiedzy i umiejętności, gdy nikt inny nie wie tego, co oni wiedzą. Niektórzy niezastąpieni pracownicy są oddani dobru swojego pracodawcy i współpracowników. Mogą wahać się przed wyjazdem na wakacje. Jeśli ich umiejętności są potrzebne z godziny na godzinę, uczestniczenie w spotkaniach komisji staje się dla nich trudniejsze. To ludzie, którzy noszą sygnalizatory i nie mogą siedzieć spokojnie nawet na dwugodzinnych zajęciach. Jeśli niezbędne umiejętności pracowników wpływają na codzienną działalność, mogą mieć trudności z wyjazdem na szkolenia, konferencje i zjazdy poza siedzibą firmy. Pomimo tego, że nadają się do awansu, niezbędne osoby mogą być opóźnione w zmianie kariery, ponieważ organizacja uważa, że szkolenie zastępców jest trudne lub kosztowne. W skrajnych przypadkach nowo awansowani menedżerowie mogą nadal wykonywać specjalistyczne obowiązki, które powinni wykonywać ich pracownicy. Czasami nawet wiceprezes operacyjny jest jedyną osobą, która może dokonać zmian w systemie produkcyjnym, które powinien wykonać programista trzy lub cztery poziomy w dół. Szczególny rodzaj niezbędności występuje wtedy, gdy pracownik staje się de facto zasobem wsparcia technicznego dla konkretnego pakietu oprogramowania lub systemu. Bez zgody przełożonych pracownicy ci mogą znaleźć się w trudnej sytuacji. Mogą zostać zwolnieni, ponieważ ich produktywność spada zbyt nisko zgodnie z ich opisem stanowiska, co nie obejmuje udzielania nieudokumentowanego wsparcia technicznego innym osobom. Mogą się wypalić i rzucić z powodu przepracowania i krytyki. Mogą też wywołać niechęć wśród swoich kolegów i sąsiadów, odmawiając im pomocy lub narzekając na przepracowanie. Ewentualnie mogą cieszyć się sytuacją i całkiem skutecznie sprostać wszystkim wymaganiom swojego czasu, dopóki inni w dziale informatycznym nie zaczną czuć się zagrożeni i ktoś albo poskarży się zwierzchnikom, albo zacznie rozpowszechniać nieprzyjemne komentarze na temat tych nieautoryzowanych technik wsparcia. Patrząc na tę sytuację z punktu widzenia zarządzania, odbiorcy tej bezpłatnej pomocy mają problemy. Im dłużej upierają się przy pozornie darmowej pomocy od swojego nieoficjalnego dobroczyńcy, tym dłużej mogą unikać poinformowania wyższej kadry kierowniczej, że potrzebują pomocy. Kiedy bańka pęka i ekspert staje się niedostępny, menedżerowie stają przed nagłym zapotrzebowaniem na nieplanowane zasoby. W większości organizacji trudno jest spełnić nieoczekiwane wymagania kadrowe. Menedżerowie mają trudności z wyjaśnieniem, dlaczego nie byli w stanie przewidzieć potrzeby i zaplanować na nią budżetu. Czasami osoby nadal są niezbędne z obawy, że ich wartość dla pracodawców tkwi w ich prywatnej wiedzy. Takim pracownikom nie podoba się szkolenie innych. Najlepszym sposobem na zmianę ich szkodliwego nastawienia jest dawanie dobrego przykładu; menedżerowie powinni dzielić się wiedzą z nimi i wszystkimi innymi

członkami swojej grupy. Edukacja powinna być normalną częścią sposobu pracy każdego w przedsiębiorstwie. Menedżerowie mogą zachęcać do cross-szkolenia, przeznaczając na to czas. Cross-szkolenie może być czynnikiem oceny pracowników. Na przykład aktualne tematy z prasy branżowej i czasopism naukowych można omawiać w klubie czasopism lub na nieformalnych, zaplanowanych spotkaniach, na których ludzie na zmianę prezentują wyniki ostatnich badań w interesujących ich obszarach. Niechęć do wyjaśniania swojej pracy komuś innemu może również maskować nieuprawnioną lub nielegalną działalność. Weźmy na przykład przypadek Lloyda Benjamina Lewisa, asystenta oficera operacyjnego w Wells Fargo Bank w Beverly Hills w Kalifornii. Umówił się z konfederatem spoza banku, aby spieniężyć fałszywe czeki do 250 000 każdy na wybranych legalnych kontach w oddziale Lewisa. Używając tajnego kodu skradzionego z innego oddziału, Lewis skrupulatnie kodował kredyt na dokładną kwotę kradzieży, dając w ten sposób złudzenie, że naprawi błąd w transakcji. Lewis ukradł swojemu pracodawcy 21,3 miliona dolarów między wrześniem 1978 a styczniem 1981, kiedy został złapany przez przypadek. Z nieznanych przyczyn program komputerowy oznaczył jedną z jego oszukańczych transakcji, aby inny pracownik został powiadomiony o nieprawidłowości. Odkrycie oszustwa nie zajęło dużo czasu, a Lewis został skazany za defraudację. Został skazany na pięć lat więzienia federalnego. Ponieważ Lewis musiał być fizycznie obecny, aby schwytać fałszywe czeki, gdy przechodziły przez system, nie mógł sobie pozwolić na to, by ktoś przy nim obserwował, co robi. Lewis byłby mniej niż entuzjastycznie nastawiony do wyszkolenia zastępcy do wykonywania swojej pracy. Gdyby ktokolwiek został przeszkolony, malwersacja prawdopodobnie nie trwałaby tak długo lub nie stałaby się tak poważna.

Postęp kariery

W temacie związanym z unikaniem niezbędności menedżerowie mogą poprawić klimat bezpieczeństwa poprzez przyjęte zasady dobrego zarządzania zasobami ludzkimi, takie jak awans zawodowy dla wszystkich pracowników. Promując osoby do nowych obowiązków, menedżerowie mogą również zwiększyć liczbę osób posiadających wiedzę specjalistyczną w zakresie funkcji krytycznych. Kiedy menedżerowie przeprowadzają regularne przeglądy wyników swoich pracowników, powinni obejmować omówienie celów zawodowych każdej osoby. Tutaj, na podstawie podsumowania sporządzonego przez eksperta ds. zatrudnienia Lee Kushnera, znajduje się kilka praktycznych pytań do omówienia z pracownikami w ramach ich rozmów kwalifikacyjnych.

1. Jakie są Twoje długoterminowe plany?

2. Jakie są Twoje mocne i słabe strony?

3. Jakie umiejętności musisz rozwinąć?

4. Czy w ciągu ostatniego roku nabyłeś nową umiejętność?

5. Jakie są Twoje najważniejsze osiągnięcia w karierze i czy wkrótce osiągniesz kolejne?

6. Czy awansowałeś w ciągu ostatnich trzech lat?

7. Jakie inwestycje poczyniłeś we własnej karierze?

Kiedy menedżerowie wspierają interesy i aspiracje jednostek, budują klimat szacunku i uznania, a jednocześnie wspierają pozytywne odczucia dotyczące organizacji.

Czas wakacji

W przykładzie przedstawionym wcześniej Lloyd Benjamin Lewis traktował swoje nieautoryzowane obowiązki (kradzież pieniędzy z banku) tak poważnie, że przez cały okres defraudacji, około 850 dni,

nigdy się nie spóźniał, nigdy nie był nieobecny i nigdy nie brał jeden dzień urlopu w ciągu ponad dwóch lat. Każdy kierownik centrum danych powinien być bardzo zaniepokojony faktem, że pracownik nie był nieobecny lub spóźnił się ani jednego dnia przez ponad dwa lata. Zazwyczaj w firmach obowiązuje zasada, że niewykorzystane dni urlopu można przenosić tylko na ograniczony czas, a następnie wygasają. Ma to być zachętą do wzięcia urlopu; dla normalnych, uczciwych pracowników prawdopodobnie działa dobrze. Dla nieuczciwych pracowników, którzy muszą być obecni, aby kontrolować oszustwo, utrata dni urlopu jest nie do zniesienia. Każdy pracownik powinien być zobowiązany do wzięcia zaplanowanych urlopów w ciągu określonego i krótkiego terminu. Nie należy zezwalać na żadne wyjątki. Nadmierny opór przed braniem urlopu powinien zostać zbadany, aby dowiedzieć się, dlaczego pracownik nalega na ciągłe przebywanie w pracy. Niestety to podejrzane podejście do perfekcyjnej frekwencji może powodować problemy dla oddanego, oddanego i uczciwego pracownika. Niewinna osoba może wpaść w sieć podejrzeń właśnie z powodu wyjątkowego zaangażowania. Tego rodzaju trudności można uniknąć poprzez:

1. Upowszechnianie uzasadnienia tej polityki przez wszystkich pracowników, aby nikt nie czuł się wyróżniony;

2. Poleganie na osądzie, dyskrecji i dobrej woli kierownika prowadzącego dochodzenie, aby uniknąć zranienia u swoich najbardziej lojalnych pracowników; oraz

3. Tymczasowe przełączanie funkcji takiego pracownika, aby sprawdzić, czy coś się zepsuje.

Reagowanie na zmiany w zachowaniu

Każde nietypowe zachowanie może wzbudzić ciekawość menedżera. Co ważniejsze z punktu widzenia zarządzania bezpieczeństwem, każda spójna zmiana zachowania powinna wzbudzać zainteresowanie. Czy normalnie punktualna osoba nagle się spóźnia, dzień po dniu? Czy pracownik zaczął regularnie pojawiać się w szytych na miarę garniturach? Dlaczego zwykle urocza osoba warczy wulgaryzmów na podwładnych w dzisiejszych czasach? Co odpowiada za to, że ktoś nagle codziennie pracuje w nadgodzinach, gdy nie ma żadnego znanego specjalnego projektu? Czy kompetentna osoba popełnia teraz oczywiste błędy w prostych raportach? Jak to się dzieje, że dawniej zadowolony z siebie pracownik jest teraz wymagającym i zgorzkniałym narzekaczem? Przy tak dużej liczbie spraw finansowych przedsiębiorstwa kontrolowanych przez systemy informatyczne, nic dziwnego, że nagłe bogactwo może być wskazówką, że ktoś popełnia przestępstwo komputerowe. Uczestnik kursu z zakresu bezpieczeństwa systemów informatycznych poinformował, że urzędnik księgowy w agencji rządowej w Waszyngtonie został aresztowany za masową defraudację. Porada? Pewnego dnia przyjechał do pracy sportowym samochodem Porsche i pochwalił się drogimi nieruchomościami, które kupował w zamożnej części regionu stołecznego – wszystko to całkowicie wykraczało poza wszelkie rozsądne oszacowania jego dochodów. Nie wszyscy złodzieje są tak głupi. Zdrowa ciekawość jest jak najbardziej uzasadniona, jeśli widzisz pracownika w niezwykle drogich ubraniach, który po latach jeździ eleganckim samochodem ze zardzewiałym wiadrem i przyjemnie rozmawia o ostatniej podróży do Acapulco, gdy jego pensja nie wydaje się wyjaśniać takich wydatków. Jednak niezamówione pytania dotyczące prywatnego życia ludzi zwykle nie przynoszą żadnych przyjaciół. Istnieje delikatna linia do przejścia, ale ignorowanie problemu nie powoduje jej zniknięcia. Inny rodzaj zmiany – w kierunku negatywnym – również może wskazywać na kłopoty. Dlaczego menedżer systemu wygląda obecnie na przygnębionego i wyświechtanego? Czy jest w ferworze osobistego kryzysu zadłużenia? W uścisku szantażysty? Dotknięty rodzinnym ratunkiem medycznym? Kompulsywny hazardzista, który ma złą passę? Z samych tylko względów humanitarnych chciałoby się wiedzieć, co się dzieje, aby pomóc; jednak kierownik zajmujący się bezpieczeństwem byłby zmuszony do zbadania sprawy. W dzisiejszych

czasach wybuchowej wściekłości i łatwego dostępu do broni ignorowanie pracowników z ciemną chmurą unoszącą się nad ich głowami może być nieodpowiedzialne i niebezpieczne.

Każda radykalna zmiana osobowości powinna budzić niepokój. Jeśli zwykle zrelaksowana główna księgowa ma teraz kropelki potu na czole za każdym razem, gdy omawiasz ścieżki audytu, być może nadszedł czas, aby dokładniej przyjrzeć się jej pracy. Dlaczego dobry człowiek z rodziny zaczyna wracać z długich obiadów z whisky na oddechu? Niegdyś ponury menedżer przechadza się teraz po biurze z wiecznym uśmiechem na twarzy. Co się stało? Albo co się dzieje? Wszystkie te zmiany powinny ostrzegać menedżerów o możliwości zmian w życiu ich pracowników. Chociaż zmiany te rzeczywiście wpływają na bezpieczeństwo organizacji, dotyczą również menedżerów jako istot ludzkich, które mogą pomagać innym ludziom. Wahania nastroju, drażliwość, depresja, euforia — to mogą być oznaki stresu psychicznego. Czy pracownik staje się alkoholikiem? Narkoman? Wykorzystywany w domu? Masz trudności finansowe? Masz problemy z nastolatkami? Zakochasz się w koleżance? Oczywiście menedżerowie nie mogą pomóc wszystkim, aw niektórych przypadkach pomoc powinna obejmować wykwalifikowanych specjalistów zdrowia psychicznego; ale przynajmniej każdy może wyrazić troskę i wsparcie w delikatny i delikatny sposób. Takie rozmowy powinny odbywać się na osobności, bez niepokojenia tematu i ekscytowania innych pracowników. W dowolnym momencie menedżer powinien swobodnie zaangażować dział HR lub personalny. Zatrudnią psychologa lub wyszkolonego doradcę na personel lub będą w stanie zapewnić odpowiednią pomoc w inny sposób, na przykład za pośrednictwem telefonicznej linii kryzysowej. Zdarzają się smutne przypadki, w których pracownicy wykazywali oznaki stresu, ale zostały zignorowane, z katastrofalnymi konsekwencjami: samobójstwa, morderstwa, kradzieże i sabotaże. Bądź czujny na wskaźniki i szybko podejmuj działania. Australijska ekspertka ds. zasobów ludzkich, Laura Stack, przedstawia tę analizę oznak skrajnego stresu: ludzie zwykle nie nagle nagle się wywracają; emitują wczesne sygnały ostrzegawcze. Na szczęście menedżerowie mogą zaobserwować oznaki stresu w zachowaniu pracowników, zaczynając od łagodniejszych objawów, a kończąc na wściekłości na biurku. Uważaj na następujące etapy stresu:

* Stan fizyczny: bóle głowy, choroba, zmęczenie.

* Faza społeczna: negatywne nastawienie, obwinianie innych, niedotrzymanie terminów, praca przez lunch.

* Faza mózgowa: obserwowanie zegara, błędy w zadaniach, drobne wypadki, roztargnienie i niezdecydowanie.

* Faza emocjonalna: złość, smutek, płacz, wrzask, uczucie przytłoczenia, depresja.

* Etap duchowy: rozmyślanie, płacz, chęć dokonania drastycznych zmian w życiu, złe relacje z ludźmi, dystansowanie się od relacji osobistych.

Praca menedżera w sondowaniu zmian w zachowaniu jest trudna; trzeba iść po cienkiej i możliwie niewidocznej linii między leseferyzmem, narażając się na żal do końca życia, a nawet oskarżenie o zaniedbanie obowiązków, a jawną ingerencję w prywatne sprawy personelu, ryzykując zawstydzenie i ewentualne oskarżenie o nękanie. Pomogą w tym spisane zasady; podobnie jak silna i ciągła współpraca z personelem HR. Wyjaśnienie wszystkim pracownikom, że menedżerowie są dostępni w celu uzyskania wsparcia, ale również oczekuje się od nich zbadania nietypowego zachowania, pomoże również uniknąć nieporozumień.

Rozdzielenie obowiązków

Te same zasady, które mają zastosowanie do kontroli pieniędzy, powinny mieć zastosowanie do kontroli danych. Kasjerzy w banku, gdy ktoś deponuje duży czek, zawsze udają się do przełożonego,

aby ta osoba obejrzała czek i zainicjowała transakcję. Kiedy kasjerzy w nocy opróżniają bankomaty i napełniają pojemniki na gotówkę, zawsze obecne są dwie osoby. W większości organizacji osoba tworząca czek nie jest osobą, która go podpisuje. W dobrze zarządzanych departamentach systemów informatycznych, przy dobrym bezpieczeństwie operacyjnym, wprowadzanie danych różni się od walidacji i weryfikacji8. bezpośredni przełożony sprawdza pracę. Nie ma usprawiedliwienia dla umożliwienia nadzorcy wprowadzania danych wprowadzenia transakcji, a następnie jej faktycznej autoryzacji. Co by było, gdyby wpis był błędny lub fałszywy? Gdzie będzie kontrola? W zapewnianiu jakości rozwoju programu zasady rozdziału obowiązków są dobrze ugruntowane. Na przykład osoba, która projektuje lub koduje program, nie może być jedyną osobą, która testuje projekt lub kod. Systemy testowe są oddzielone od systemów produkcyjnych; programiści nie mogą mieć dostępu do poufnych i krytycznych danych kontrolowanych przez personel produkcyjny. Programiści nie mogą wchodzić do sali komputerowej, jeśli nie mają tam autoryzowanych interesów; operatorzy nie mogą modyfikować programów produkcyjnych i zadań wsadowych bez zezwolenia. Menedżerowie powinni rozważyć rezygnację z dostępu do funkcji delegowanych dwóm lub więcej podwładnym. Utrzymanie takiego dostępu może spowodować więcej problemów niż rozwiązać, ale w sytuacji awaryjnej dostęp i kontrolę można łatwo przywrócić. Taka postawa jest przykładem koncepcji rozdziału obowiązków. Na początku 1995 roku światem finansów wstrząsnął upadek firmy bankowości inwestycyjnej Barings PLC. Szef biura w Singapurze, Nicholas Leeson, został oskarżony o grę na rynku kontraktów terminowych z katastrofalnymi konsekwencjami. Istotne jest to, że wszystkie zlecenia udało mu się wykonać bez niezależnego przeglądu. Gdyby nastąpiło skuteczne rozdzielenie obowiązków, upadek by nie nastąpił. Kolejny szokujący przykład miał miejsce, gdy administrator systemu w UBS PaineWebber, zdenerwowany kiepską premią płacową, którą otrzymał, wdrożył złośliwy kod w sieci firmy. Ale zanim rzucił pracę, napisał program, który usuwał pliki i siał spustoszenie w sieci firmy. Tworząc bombę logiczną, był w stanie uderzyć w ponad 1000 serwerów i 17 000 pojedynczych stacji roboczych. Dodatkowo, kupując puty przeciwko UBS, zyskałby na tym ataku. Powiązane podejście nazywa się podwójną kontrolą. Jako przykład podwójnej kontroli rozważ odwieczny problem posiadania tajnych haseł nieznanych menedżerom, którzy czasami potrzebują awaryjnego dostępu do tych haseł. Ten problem na ogół nie dotyczy haseł zwykłych użytkowników, które zwykle mogą zostać zresetowane przez administratora bezpieczeństwa bez konieczności znajomości starego hasła. To tymczasowe hasło powinno zostać zmienione przez użytkownika na naprawdę tajny ciąg znaków po jednokrotnym zalogowaniu. Jednakże, aby zabezpieczyć się przed nieobecnością jedynej osoby, która ma hasło roota do systemu, prawdopodobnie dlatego, że inni są na wakacjach, zaleca się zorganizowanie podwójnego dostępu do kopii zapasowych hasła. Zasada podwójnej kontroli nakazuje, aby taka kopia hasła roota była dostępna tylko wtedy, gdy dwóch funkcjonariuszy organizacji jednocześnie podpisuje się pod nią podczas wyjmowania jej z bezpiecznego magazynu:

* Można przechowywać pisemną kopię hasła roota w naprawdę nieprzejrzystej kopercie, zapieczętować ją, podpisać pieczęć, zakleić pieczęć nieusuwalną taśmą, a następnie przechowywać kopertę w firmowym sejfie lub sejfie

* Hasło można zaszyfrować dwukrotnie za pomocą kluczy publicznych dwóch funkcjonariuszy; podwójne szyfrowanie wymaga od funkcjonariuszy odszyfrowania zaszyfrowanego tekstu w odwrotnej kolejności szyfrowania

Podsumowując, menedżerowie powinni zastanowić się nad strukturą kontroli nad informacją podczas projektowania polityk bezpieczeństwa, tak aby zabezpieczenia zapewniane przez oddzielenie obowiązków lub podwójną kontrolę były obecne we wszystkich systemach.

Macierze zdolności i odpowiedzialności

Jednym z narzędzi, które mogą pomóc w ocenie i poprawie odporności organizacji, jest macierz możliwości. Najpierw należy wymienić (lub przeprowadzić burzę mózgów, być może przy użyciu Computer-Aided ConsensusTM) wszystkich krytycznych funkcji wymaganych przez organizację oraz wszystkich osób w zespole. Następnie grupa musi zdecydować o sposobie oceny zdolności każdej osoby; rysunek sugeruje jeden sposób, aby to zrobić, ale w żadnym wypadku nie ma to na celu ograniczania użytkowników. Grupa może dojść do konsensusu co do tego, który z członków zespołu może wykonać jakie zadania na jakim poziomie kompetencji, a następnie zbadać ogólny wzorzec umiejętności. Dowód 45.1 pokazuje taką matrycę z wymyślonymi informacjami. Problemy mogą być uwidocznione, gdy nikt nie ma wysokich umiejętności lub gdy zbyt mało osób może skutecznie wykonywać te zadania. Innym problemem jest to, że niektórzy ludzie mogą mieć tak dużo wiedzy w porównaniu z innymi, że organizacja jest w niebezpieczeństwie, gdyby byli nieobecni; takie przypadki powinny prowadzić do wysiłków szkoleniowych mających na celu podniesienie innych do odpowiedniego poziomu wiedzy i umiejętności. Poszczególnym osobom może również wyraźnie brakować umiejętności; znowu szkolenie może pomóc rozwiązać takie problemy. Należy opracować podobną macierz pokazującą obowiązki każdego członka zespołu, ze wskaźnikami, kto ponosi główną odpowiedzialność i nazwiskami dwóch lub więcej członków, którzy mogą służyć jako kopie zapasowe (w kolejności priorytetów). Ważne, aby każdy członek zespołu samodzielnie wypełnił swoją matrycę, ponieważ konflikty mogą zostać wykryte w ten sposób. Macierz odpowiedzialności może identyfikować problemy w strukturze zarządzania. Na przykład

* Niektóre zadania mogą być formalnie nie przydzielone lub nikt nie ma przypisanej głównej odpowiedzialności, co prowadzi do awarii w odpowiedzi, zwłaszcza w sytuacjach awaryjnych.

* Mogą istnieć zadania, w których dwie lub więcej osób uważa, że są głównymi decydentami lub liderami zadania, co prowadzi do konfliktów.

* Niektóre osoby mogą być utożsamiane ze zbyt wieloma przydzielonymi zadaniami; inni mogą mieć za mało.

Brak nieautoryzowanych sond bezpieczeństwa

Ogólnie rzecz biorąc, wszyscy menedżerowie – nie tylko specjaliści ds. bezpieczeństwa – powinni zawsze szukać słabych punktów i możliwości poprawy bezpieczeństwa. Jednak nikt nigdy nie powinien testować systemów produkcyjnych pod kątem podatności bez pełnej współpracy korporacyjnej grupy ochrony informacji i tylko za zgodą odpowiednich kierowników. Pisemna zgoda na jawne testy bezpieczeństwa jest nieformalnie znana jako karty wyjścia z więzienia, ponieważ bez nich pracownicy mogą trafić do więzienia za nieautoryzowane próby bezpieczeństwa systemu.

Przypadek Randala Schwartza, konsultanta Intel Corporation w Beaverton w stanie Oregon, jest dla pracowników zbawiennym przykładem niebezpieczeństwa nieautoryzowanych sond bezpieczeństwa. Został skazany za włamanie się do sieci komputerowych Intel Corporation, co, jak twierdził, było próbą wykrycia luk w zabezpieczeniach, gdy pracował tam jako konsultant. Niedoszły ekspert ds. bezpieczeństwa nie powiadomił swoich pracodawców o swoich zamiarach i zapomniał uzyskać upoważnienie do kradzieży haseł i dokonywania nieautoryzowanych zmian w oprogramowaniu systemowym. Został skazany za trzy przestępstwa w lipcu 1995 roku i został ukarany grzywną w wysokości 68 000 dolarów w ramach restytucji, a także został objęty pięcioletnim okresem próbnym i musiał wykonać 480 godzin prac społecznych. Kontrprzykładem ostrzegającym menedżerów przed niewłaściwą gorliwością w tłumieniu współpracy z organami ścigania jest przypadek Shawna Carpentera, analityka bezpieczeństwa wykrywania włamań do sieci w Sandia National Laboratories. Został zwolniony przez nieśmiałych administratorów, gdy pracował z funkcjonariuszami organów ścigania w celu wyśledzenia rozległej penetracji zasobów bezpieczeństwa narodowego USA.

Dochodzenie o kryptonimie TITAN RAIN rozpoczęło się pod koniec 2003 roku. Carpenter zauważył powódź eksperckiej aktywności hakerskiej skupiającej się w sprawie kradzieży danych pochodzących z szerokiego zakresu interesów bezpieczeństwa narodowego. Carpenter odkrył, że „ataki pochodziły z zaledwie trzech chińskich routerów, które działały jako pierwszy punkt połączenia sieci lokalnej z Internetem". Carpenter współpracował z kontrwywiadem armii amerykańskiej i śledczymi FBI, aby dowiedzieć się więcej o atakach i napastnikach. Carpenter nigdy nie wykorzystywał w swoich śledztwach sprzętu ani zasobów sieciowych Sandii ani należących do rządu. Administratorzy zastosowali dyrektywę Sandia Internal Directive 12 ISNL ID012, która „szczególnie zabrania pracownikom rozmawiania z urzędnikami lokalnymi, stanowymi lub federalnymi". W 2007 roku Carpenter otrzymał 4,3 miliona dolarów za bezprawne rozwiązanie umowy. W lutym 2012 r. policja i dyrektorzy sądów w Wiedniu w Austrii zorganizowali teatralnie przekonujący atak terrorystyczny jako ćwiczenie szkoleniowe. Inscenizacja obejmowała „jedną symulowaną śmierć, podobno strzałem w głowę. Do symulacji obrażeń użyto makijażu, a kilku funkcjonariuszy umieszczono w budynku tak, jakby byli osobami rannymi. Rzekoma śmierć została zainscenizowana na oczach pracowników sądu, którzy ewakuowali biura". Ponieważ żaden ze zwykłych członków personelu nie został poinformowany (i nic nie zostało ogłoszone opinii publicznej), „Następnego dnia 40 członków personelu było leczonych z powodu poważnego urazu, a nieujawniona liczba wzięła udział w zwolnieniu lekarskim. Musimy założyć, że niektórzy będą cierpieć na zespół stresu pourazowego (PTSD) w nadchodzących tygodniach i miesiącach".

ROZWIĄZANIE STOSUNKU PRACY

Biorąc nasz mandat w zakresie bezpieczeństwa w najszerszym znaczeniu, musimy chronić naszego pracodawcę i siebie przed potencjalną szkodą ze strony nieetycznych, niezadowolonych lub niekompetentnych pracowników oraz przed konsekwencjami prawnymi niewłaściwych procedur zwalniania. Zdrowy rozsądek i przyzwoitość przemawiają za humanitarnym i wrażliwym traktowaniem zwalnianych i rezygnujących. Zwalnianie ludzi to stresujący czas dla wszystkich zainteresowanych i zwykle prowadzi do zwiększonego zagrożenia bezpieczeństwa. Menedżerowie powinni zrobić wszystko, co w ich mocy, aby zapewnić uprzejme, pełne szacunku i wspierające doświadczenie podczas rozwiązywania stosunku pracy.

Rezygnacje

Potencjalnie najbardziej niebezpieczną formą rozwiązania stosunku pracy jest rezygnacja. Problem jest podsumowany w podpisie do karykatury, w której toczy się dziki atak na płonące średniowieczne miasto; wódz wojny klanów konfrontuje się z przypalonym i brudnym wojownikiem. „Nie, nie, Thorze! Plądruj, a NASTĘPNIE spłoń!" Podobnie jak wódz wojenny, pracownicy rzadko rezygnują bez planowania. Pracownik może mieć czas nieokreślony, w którym akcja jest nieuchronna, podczas gdy pracodawca może pozostać nieświadomy sytuacji. Jeśli pracownik ma złe uczucia lub złe zamiary wobec obecnego pracodawcy, następuje okres podatności na zagrożenia, często nieznany kierownictwu. Nieuczciwi lub niezrównoważeni pracownicy mogą ukraść informacje lub sprzęt, spowodować natychmiastowe lub opóźnione szkody za pomocą technik programowych lub wprowadzić błędne dane do systemu. Zasady omówione w poprzednich częściach tego rozdziału powinny ograniczać ryzyko związane z rezygnacją. Celem menedżera powinno być, aby rezygnacje były rzadkie i rozsądne. Pozostając w kontakcie z uczuciami, nastrojami i morale pracowników, menedżerowie mogą zidentyfikować źródła napięcia i być może rozwiązać problemy, zanim doprowadzą one do rezygnacji i związanego z nimi zagrożenia bezpieczeństwa.

Wypalanie

Zwolnienia wydają się dawać przewagę pracodawcom, ale mogą być komplikacjami.

Czas

Jedną z zalet jest możliwość kontrolowania czasu powiadomienia zwalnianego pracownika, aby zminimalizować wpływ na organizację i jej działalność. Na przykład pracodawcy mogą uznać za najlepsze zwolnienie niekompetentnego lub nieakceptowalnego pracownika przed rozpoczęciem nowego ważnego projektu lub po jego zakończeniu. Niektórzy twierdzą, że aby zmniejszyć psychologiczny wpływ na innych pracowników, powinni zwalniać pracowników pod koniec dnia, być może nawet przed długim weekendem. Teoria jest taka, że praktyka daje każdemu czas na odstąpienie od pracy poza godzinami pracy. Ci menedżerowie twierdzą, że nie chcą, aby gwar rozmów i spekulacji, które często pojawiają się po zwolnieniu, przeszkadzał w pracy. Ta polityka nie uwzględnia stresu psychicznego pracowników, którzy mają zepsuty weekend i nie reagują konstruktywnie na potencjalnie katastrofalną utratę regularnych dochodów. Lepszym podejściem do tego stresującego zadania jest zwolnienie pracowników w poniedziałek rano w celu przeprowadzenia nieśpiesznej rozmowy końcowej i, w razie potrzeby, doradztwa zawodowego, aby pomóc pracownikowi przygotować się do poszukiwania pracy. W tym scenariuszu godna ubolewania (z punktu widzenia menedżera) konieczność rozwiązania stosunku pracy jest buforowana przez specjalistów z działu HR, którzy mogą dać odchodzącemu pracownikowi poczucie nadziei oraz praktycznego i emocjonalnego wsparcia w tym trudnym czasie. Humanitarne podejście jest szczególnie ważne podczas redukcji lub gdy zakłady są zamykane, a wiele ludzie jest zwalnianych – jedno z najgorszych możliwych doświadczeń zarówno dla pracowników, jak i menedżerów oraz wydarzenie, które ma poważne konsekwencje dla bezpieczeństwa. W jednej z dużych firm dział personalny poprosił swoich pracowników ochrony informacji o zawieszenie kodów dostępu dla ponad 100 osób, które miały zostać zwolnione we wtorek o 18:00. W środę o 8:00 pracownicy ochrony zaczęli odbierać telefony z pytaniem, dlaczego identyfikatory logowania dzwoniących już nie działają. Okazało się, że personel personalny nie poinformował na czas zwolnionych pracowników. Trauma psychologiczna zarówno dla pracowników, którzy zostali zwolnieni, jak i dla pracowników ochrony była surowa. Kilku pracowników ochrony zostało wysłanych do domu we łzach, aby odzyskać siły po niefortunnym doświadczeniu. Szkoda wyrządzona zwolnionym pracownikom była jeszcze większa, a wpływ na morale pozostałych pracowników okazał się katastrofą. W tej sytuacji mogła dojść do przemocy.

Procedury po rozwiązaniu

Zarówno w przypadku rezygnacji, jak i zwolnień konsultanci ds. bezpieczeństwa jednogłośnie doradzają natychmiastowe działanie. Nie dla nich spokojny okres karencji, podczas którego pracownicy kończą swoje projekty lub przekazują je innym członkom personelu. Funkcjonariusze ochrony to trudna grupa i zwykle radzą taki scenariusz: Podczas formalnej rozmowy końcowej, w obecności co najmniej dwóch kierowników, funkcjonariusz pracodawcy informuje pracownika uprzejmie, że jego zatrudnienie dobiega końca. Podczas rozmowy wyjazdowej funkcjonariusz wyjaśnia przyczyny rozwiązania stosunku pracy. Funkcjonariusz wręcza pracownikowi czek za okres wypowiedzenia wymagany przepisami prawa lub umową wraz z należną odprawą. Pod nadzorem, najlepiej w obecności co najmniej jednego pracownika ochrony, pracownik jest eskortowany do przyzwyczajonego miejsca pracy i proszony o zabranie wszystkich rzeczy osobistych i umieszczenie ich w kontenerze zapewnionym przez pracodawcę. Pracownik zwraca wszystkie identyfikatory firmowe, identyfikatory, wizytówki, karty kredytowe i klucze, a następnie jest grzecznie wyprowadzany na zewnątrz budynku. W tym samym czasie wszystkie ustalenia dotyczące bezpieczeństwa muszą zostać zmienione, aby wykluczyć byłego pracownika z dostępu do budynku i wszystkich systemów informatycznych. Takie ograniczenia mogą obejmować:

* Usunięcie nazwiska osoby ze wszystkich list posterunków bezpieczeństwa autoryzowanego dostępu

* Wyraźne informowanie strażników, że były pracownik nie może zostać wpuszczony do budynku bez opieki lub w towarzystwie pracownika, bez specjalnego upoważnienia ze strony wyznaczonych władz

* Zmiana kombinacji, przeprogramowanie systemów kart dostępu i wymiana kluczy fizycznych, jeśli to konieczne, we wszystkich bezpiecznych obszarach, do których dana osoba miała autoryzowany dostęp

* Usunięcie lub zmiana wszystkich osobistych kodów dostępu, o których wiadomo, że były używane przez byłego pracownika we wszystkich zabezpieczonych systemach komputerowych, w tym mikrokomputerach, sieciach i komputerach typu mainframe

* Informowanie wszystkich zewnętrznych agencji (np. magazynów taśmowych i funkcji zleconych na zewnątrz), że były pracownik nie jest już upoważniony do uzyskiwania dostępu do jakichkolwiek informacji pracodawcy lub do inicjowania procedur bezpieczeństwa lub odzyskiwania po awarii

* Prośba o współpracę zewnętrznych agencji w informowaniu pracodawcy o próbach pełnienia przez pracowników nieuprawnionych funkcji w imieniu byłego pracodawcy

Zadanie jest utrudnione przez staż pracy lub jeśli były pracownik odegrał ważną rolę w odzyskiwaniu danych po awarii lub bezpieczeństwie. Pracodawca powinien wytrwale wyszukiwać wszystkie możliwe drogi wjazdu wynikające z zajmowanego stanowiska i znajomości procedur bezpieczeństwa. W jednej z historii krążącej w literaturze dotyczącej bezpieczeństwa pracownik został zwolniony bez właśnie sugerowanych zabezpieczeń. W następną sobotę wrócił do pracy swoim kombi i powitał ochroniarza ze zwykłą życzliwością i pewnością siebie. Strażnik, który znał go od lat, nie wiedział, że mężczyzna został zwolniony. Były pracownik nadal miał kody dostępu i kopie kluczy do bezpiecznych obszarów. Wszedł do pokoju komputerowego bez nadzoru, zniszczył wszystkie pliki w systemie, a następnie otworzył sejf taśm. Zaangażował strażnika do pomocy w załadowaniu wszystkich taśm zapasowych firmy do swojego kombi. Złodziej narzekał nawet, że musi pracować w weekendy. Ten przestępca próbował następnie wyłudzić pieniądze od firmy, grożąc zniszczeniem taśm zapasowych, ale został znaleziony przez policję i aresztowany na czas, aby zapobiec katastrofie swojego byłego pracodawcy. Ta historia podkreśla wagę dotarcia do wszystkich, którzy muszą wiedzieć, że pracownik nie pracuje już dla przedsiębiorstwa.

Wsparcie w przypadku przymusowych wypowiedzeń

Bezpieczeństwo czasami uniemożliwia przyjęcie pożegnalne, co jest oczywistym znakiem życzliwości. Problem z imprezą pożegnalną w pracy polega na tym, że pracownicy wychodzący pod chmurę mogą czuć się upokorzeni, gdy inni ludzie biorą udział w imprezie, ale tego nie robią. Ogólnie rzecz biorąc, rozsądne jest traktowanie wszystkich odchodzących pracowników tak samo, nawet jeśli wypowiedzenie jest niedobrowolne. Nic jednak nie stoi na przeszkodzie, by humanitarny i wrażliwy pracodawca zachęcał pracowników do zorganizowania imprezy po godzinach pracy nawet dla osób, które zostały zwolnione. Jeśli jednak rezygnacja jest na dobrych warunkach, pracodawca może nawet zorganizować uroczystość, być może w godzinach pracy i być może na koszt firmy, nie martwiąc się o ewentualne negatywne konsekwencje. Zwolnienie lub rezygnacja na złych warunkach niesie ze sobą dwa zagrożenia psychologiczne: skutki zakłopotania, wstydu i złości na daną osobę oraz skutki plotek, urazy i strachu na pozostały personel. Oba rodzaje problemów można zminimalizować, publikując procedury wypowiedzenia w dokumentach organizacyjnych przekazywanych wszystkim pracownikom; poprzez wymaganie od wszystkich pracowników podpisania oświadczenia potwierdzającego zapoznanie się i zgodę na procedury wypowiedzenia; oraz konsekwentne stosowanie procedur rozwiązania. Osobisty szok wywołany zwolnieniem można złagodzić uprzejmością i rozwagą zgodną z naturą powodów zwolnienia, chociaż nawet nieprzyjemni ludzie nie powinni być narażeni na słowne lub fizyczne znęcanie się, bez względu na to, jak złe ich zachowanie. Ich traktowanie powinno być

zgodne z tym wymierzanym innym zwolnionym pracownikom, a jeśli to możliwe, powinny istnieć hojne odprawy. Zamieszanie organizacyjne można zmniejszyć, zwołując zebrania całej organizacji lub wydziałów, aby poinformować pozostałych pracowników o szczegółach znaczącego rozwiązania stosunku pracy. Pomocne mogą być otwarte dyskusje, w tym o tym, jak ludzie myślą o zerwaniu relacji. Pozostali pracownicy mogą cierpieć smutek jako proces, a nie stan. Żal jest normalną i zdrową reakcją na zerwanie relacji (np. śmierć bliskiej osoby, rozwód, a nawet utratę współpracownika). Niektórzy ludzie cenią relacje społeczne bardziej niż inne aspekty swojej pracy, a zwolnienia mogą szczególnie na nich wpływać. Smutek obejmuje etapy zaprzeczenia, gniewu, żałoby i powrotu do zdrowia. Próba zapobieżenia takim reakcjom poprzez zaprzeczanie, że ludzie słusznie mają uczucia, jest głupia i przynosi efekt przeciwny do zamierzonego. O wiele lepiej jest zachęcać tych, którzy są zdenerwowani, do wyrażania swoich uczuć i angażowania się w konstruktywną dyskusję, niż tłumić w daremnej próbie stłumienia dyskusji.

Styl wypowiedzenia

Sposób, w jaki organizacja radzi sobie z rozwiązaniem stosunku pracy, wpływa nie tylko na relacje wewnętrzne; wpływa również na jej wizerunek w świecie zewnętrznym. Potencjalni pracownicy dwa razy zastanowią się nad przyjęciem ofert pracy od organizacji, która źle traktuje odchodzących pracowników. Klienci mogą wywrzeć negatywne wrażenie stabilności firmy, jeśli nadużywa ona własnych ludzi. Inwestorzy mogą również spojrzeć krzywo na firmę, która cieszy się reputacją tandetnego traktowania pracowników. Złe relacje między menedżerami i pracownikami są sygnałem ostrzegawczym przed długofalowymi trudnościami.

Kwestie prawne

Istnieje inny wymiar rozwiązania stosunku pracy, który zależy od lokalnych przepisów i środowiska postępowania sądowego. Na przykład Stany Zjednoczone są uważane za jeden z najbardziej spornych narodów na świecie, być może z powodu dużej liczby prawników w porównaniu z całkowitą populacją. Poniższa lista nie jest poradą prawną; w celu uzyskania porady prawnej skonsultuj się z prawnikiem. Jednak proste doświadczenie uczy pewnych zasad, nawet bez studiowania prawa. Oto kilka pragmatycznych wskazówek dotyczących zapobiegania problemom prawnym związanym ze zwolnieniami z przyczyn:

* Zbuduj solidną, udokumentowaną sprawę do zwolnienia kogoś przed podjęciem działania.

* Prowadź dobre zapisy, bądź obiektywny i uzyskaj opinie kilku godnych zaufania osób.

* Zaoferuj przestępcy pracownikowi wszelkie uzasadnione szanse na poprawienie jego zachowania.

* Przekaż pracownikowi jasną opinię na długo przed rozważeniem zwolnienia.

Czas jest ważny w relacjach pracowniczych, podobnie jak we wszystkim, co robimy. W szczególności, jeśli okaże się, że pracownik zachowuje się niewłaściwie lub nielegalnie, nie może wystąpić znaczne opóźnienie w rozwiązaniu problemu. Takie osoby mogłyby pozwać pracodawcę i poszczególnych menedżerów. Mogli argumentować w sądzie, że sam fakt opóźnienia w ich zwolnieniu był dowodem, że zwolnienie było spowodowane innymi czynnikami, takimi jak konflikty osobowości, rasizm lub seksizm. Dobrze zdefiniowana procedura przejścia przez decyzję zminimalizuje takie problemy. Kluczową kwestią prawną jest spójność. Jeśli zasady takie jak te właśnie opisane na dzień zwolnienia są stosowane przypadkowo, łatwo mogą być podstawy do narzekania i niesprawiedliwości. Ci, wobec których zasady były ściśle przestrzegane, słusznie czuliby się bezwarunkowo krytykowani. Jak byśmy się czuli, gdybyśmy zostali wyróżnieni, gdy strażnicy sprawdzili, co zabraliśmy do domu z naszego biurka - gdyby wszyscy inni dostali przyjęcie i dwa tygodnie wypowiedzenia? Taka niespójność byłaby

podstawą do wszczęcia postępowania sądowego o zniesławienie. Firma może przegrać i może wygrać, ale który nieprawnik chce spędzić czas w sądzie? Kolejną kwestią, która pojawia się w związku ze zwolnieniami i rezygnacjami, są umowy o zachowaniu poufności. Wszystkie takie umowy muszą być zawarte w umowie podpisanej przed rozpoczęciem pracy przez potencjalnego pracownika; prawie niemożliwe jest zmuszenie dotychczasowego pracownika do podpisania takiej umowy. Menedżerowie, dział prawny i dział personalny powinni zbadać konieczność i wykonalność ustanowienia prawnie wiążącego zobowiązania umownego w celu ochrony poufnych informacji firmy przez określony czas po odejściu. Zazwyczaj nie nakłada się na ludzi nieokreślonych knebli, ponieważ jeden rok wydaje się normalny. (Są jednak wyjątki. Oprah Winfrey nalega, aby wszyscy pracownicy pracujący w Harpo podpisali dożywotnią umowę o zachowaniu poufności, którą podtrzymał sąd apelacyjny w Illinois, gdy były pracownik próbował napisać książkę o mediach , mogul.) Aby środek ten miał sens, pierwotna umowa o pracę powinna przewidywać, że odchodzący pracownicy muszą ujawnić swojego nowego pracodawcę, jeśli taki istnieje w tym czasie. Umowy o zakazie konkurencji wymagają od pracownika powstrzymania się od pracy dla bezpośrednich konkurentów przez około rok po ustaniu stosunku pracy. Kluczem do udanej klauzuli jest tutaj ścisła, operacyjna definicja „bezpośrednich konkurentów". Ponieważ to ograniczenie może być uciążliwą przeszkodą w zarabianiu na życie, wiele jurysdykcji zabrania takich klauzul.

STRESZCZENIE

Oto niektóre z kluczowych zaleceń :

*Wynajmowanie

* Zbadaj dokładność życiorysu każdego prawdopodobnego kandydata do pracy.

* Wykonuj dochodzenia w tle podczas zatrudniania na wrażliwe stanowiska.

* Zapewnij doświadczonym pracownikom rozmowę kwalifikacyjną z kandydatami i omówienie niespójności.

* Wymagaj podpisania odpowiedniej prawnie umowy o pracę.

* Zarządzanie bieżące

* Zidentyfikuj i rozwiąż okazje do nadużyć.

* Przydziel funkcje dostępu na podstawie potrzeb, a nie statusu społecznego.

* Zidentyfikuj niezbędnych pracowników i zorganizuj szkolenie krzyżowe innych pracowników.

* Wymagaj od pracowników urlopu lub okresowej rotacji stanowisk pracy, aby zapewnić ciągłość działania i jako możliwe wskazanie oszustwa.

* Zauważaj i reaguj na nagłe zmiany w zachowaniu i nastroju; odpowiednio zaangażować zasoby ludzkie.

* Egzekwuj rozdział obowiązków i podwójną kontrolę wrażliwych funkcji.

* Nie angażuj się ani nie toleruj nieautoryzowanych prób bezpieczeństwa systemu.

* Rozwiązanie stosunku pracy

* Zapewnij zwolnionym pracownikom możliwość uzyskania porad i wsparcia.

* Upewnij się, że dział HR współpracuje z grupą informatyczną w celu podjęcia wszelkich odpowiednich środków bezpieczeństwa, gdy ktokolwiek odchodzi z pracy w przedsiębiorstwie.

* Upewnij się, że strzały nie powodują długotrwałych problemów z morale.

* Postępuj zgodnie ze wskazówkami radcy prawnego, aby uniknąć bezprawnych procesów o zwolnienie.

* Używaj prawnie odpowiednich klauzul o zakazie ujawniania i zakazu konkurencji w umowach o pracę.

Podsumowując, bezpieczeństwo informacji zależy od koordynacji z personelem HR w celu zapewnienia spójnych zasad zatrudniania, bieżącego zarządzania i rozwiązania stosunku pracy.