Rozbić szybę w sytuacji awaryjnej

Wendell zadzwonił. Telefon zadzwonił. Brak odpowiedzi. Gdzie do cholery był Kiron? „Nie odbiera" – powiedział z frustracją Wendell. Jakub zmarszczył nos. „Myślę, że w tym tygodniu jest na jakiejś konferencji networkingowej. Pewnie dlatego. Wendell prychnął. Kiron z pewnością wybrał tydzień na nieobecność – w samym środku gigantycznego wyłomu. „No cóż, potrzebujemy hasła. Pójdę po Mike'a. Mike przyszedł minutę później, niosąc dziennik, który zwykle trzymał na biurku. Miał kilka haseł dotyczących stłuczenia szyby, na wypadek takiej ewentualności. – Proszę bardzo, Wendell. Wendell nie uważał, że jest najlepszą osobą do obsługi zapory ogniowej. Niemniej jednak skanował stronę, aż znalazł hasło dostępu administratora sieci. Wpisał go w interfejsie internetowym. Złe hasło, narzeka interfejs. Alex pstryknął palcami. „Och, zespół sieciowy zaczął używać portfela haseł. Mike, ta lista jest nieaktualna. Twarz Mike'a poczerwieniała. – Cóż, ktoś powinien był mi powiedzieć. A jakie jest hasło do portfela?" Aleks zamrugał. "Nie wiem. Kiron może to gdzieś mieć. Mamrotając do siebie, Mike odszedł. Wendell zorientował się, że nerwowo stuka w biurko. Wczoraj wieczorem pracował do późna w nocy i nie był zbyt szczęśliwy, że przyszedł do pracy tylko po to, by znaleźć się po uszy w poważnym wypadku. Nikt tak naprawdę nie znał jeszcze szczegółów, ale wyglądało to poważnie, co frustrowało go jeszcze bardziej. Chciał pomóc rozwiązać problem tak szybko, jak to możliwe i mieć już to za sobą. Ostatnią rzeczą, jakiej potrzebował, były te małe foobary, takie jak zagubione hasło. „Rozumiem" – krzyknął Mike z drugiego końca korytarza, wracając w pośpiechu. „Hasło do portfela zostało zapisane na dole zadrukowanej kartki, którą Kiron trzyma pod klawiaturą". „Ci goście z sieci są przebiegli, mówię ci" – szepnął Jacob. Wendell zjeżył się. Jacob był zbyt wesoły. W końcu to on odpowiadał za produkcyjne bazy danych. Tymczasem Mike przejął klawiaturę i teraz, gdy już mieli dostęp do portfela, gorączkowo zapisywał hasła uprawnień do różnych typów systemów. „OK, Wendell, zrobię kilka kopii tych dokumentów i rozdam je osobom, które ich potrzebują. Zapisz proszę, komu przekazujesz każde hasło." Wendell wziął papier, upewnił się, że tekst jest czytelny, a następnie podszedł do maszyny drukarskiej w północnym rogu piętra. Przyszedł i zaczął ciąć kopie na paski, tak aby na każdym pasku znajdowało się tylko jedno hasło. „A więc hasło do bazy danych, to do…" „Nie potrzebujemy tego" – przerwał nagle Jacob. „Już to wiem. Po prostu mi to daj; Zniszczę to na kawałki, żebym nie musiał później zmieniać". Alex podszedł i spojrzał na listę ponad ramieniem Wendella. „Ponieważ jesteś zajęty, wezmę hasło do zapory ogniowej. Mogę też zająć się serwerami plików. Belindzie? Skinęła głową. "Jasne. Popracuję nad przywróceniem kopii zapasowych z ostatniej nocy. Nie potrzebuję do tego żadnego hasła. „Po prostu daj mi całą listę" – powiedział spokojnie Henry. „Będę potrzebował kilku z nich do maszyn wirtualnych i systemów laboratoryjnych". „Sprawdzę serwery produkcyjne, żeby się upewnić, że wszystko działa. Chyba użyję do tego hasła konsoli lokalnej." Elwood uśmiechnął się do Wendella, odrywając dolną część oryginalnej listy haseł. Mostek telefoniczny zaćwierkał. „Jestem tutaj" – powiedział Gopal, w końcu dając się poznać na linii alarmowej. „Cześć, Gopal" – powiedział Mike i świadomie pokiwał głową, gdy Alex pomyślnie zalogował się do konsoli internetowej zapory sieciowej. „Połowa reguł zapory sieciowej jest złamana" – mruknął Alex. „Zamierzam usunąć ich." Wendell próbował podzielić swoją uwagę pomiędzy rozdawanie pasków papieru i sprawdzanie, co wszyscy robią. Czy nie powinniśmy skorzystać z zarządzania konfiguracją?" "Nie ma na to czasu. Zrobię to ręcznie" – odpowiedział Alex. Nie mając już papieru do rozdania, Wendell usiadł u boku Jacoba i obserwował pracę swojego kolegi. Poczuł się trochę nieswojo, że nie ma wystarczającej wiedzy i znajomości systemu, i czuł, że mógłby zrobić więcej, aby pomóc. "Co tu się stało?" Jacob prychnął, uderzając w klawiaturę. „Moje zmiany w konfiguracji zniknęły!" „Narzędzie do zarządzania konfiguracją nadpisało twoją zmianę" – odezwał się Henry z drugiego końca pokoju. „To będzie się zdarzać co 15 minut. Jak nazywa się ten serwer, zatrzymam go teraz. I ty też, Alex, chyba że chcesz od nowa wprowadzać te same zmiany. Jakub zmarszczył brwi. „To DB01. Ale to nie jedyny problem. Wartości domyślne nie są takie, jakich się spodziewałem." Wendell rozpoczął dochodzenie. „Hm. Wygląda na to,

że Gopal także pracuje nad DB01. Wcześniej dokonał aktualizacji. Może kończy konfigurację. Gopal, jesteś jeszcze na moście? Gopala?" Brak odpowiedzi. „Czekaj, dlaczego dokonujemy aktualizacji teraz?" zapytał Mike. Aleks wzruszył ramionami. „Zapytaj Gopala". „OK, chłopaki, musimy to powstrzymać. Rozwiążemy problem później. Na razie musimy zatrzymać ruch sieciowy". „Wyłączyłem wszystkie testowe maszyny wirtualne i maszyny laboratoryjne, więc jedyny dostęp do bazy danych jest przez Internet" – powiedział Henry. Daniel siedział spokojnie w kącie sali konferencyjnej. „Usunąłem niektóre aplikacje do analizy statystycznej, które mieliśmy w bazie danych, na wypadek, gdyby powodowały jakiekolwiek problemy". „Myślę, że wiem, jak to rozwiązać…", mruknął Gopal na linii. „Elwood mówi, że w razie potrzeby może wyciągnąć kable" – poinformował ich Mike, patrząc na swój telefon. „Nasza administracyjna sieć VLAN jest kierowana przez ten sam przełącznik, co sieć zewnętrzna" – wyjaśnił Alex, wciąż zajęty regułami zapory sieciowej. – Więc lepiej, żeby nas nie rozłączył. Mike ponownie to napisał. „Zatrzymajmy po prostu bazę danych, a ja rozpocznę przywracanie" – oznajmiła Belinda. "Nie? Nie!" Jakub krzyknął. "NIE. Nie możesz tego zatrzymać. Generujemy ważny raport i jeśli go teraz zatrzymamy, może dojść do korupcji". "Co to za różnica?" Cezar sprzeciwił się. „I tak będziemy przywracać." Jakub zacisnął zęby. „Od ostatniej nocy to ponad 50 milionów rekordów. Jeśli teraz je przywrócimy, nigdy nie dowiemy się, jakie to były zapisy.Najpierw musimy dokończyć raport. „Gopal, jakieś postępy? Mówiłeś, że możesz coś wiedzieć… – zapytał Wendell. Brak odpowiedzi. Alex zrobił krzywą minę. „Więc złamaliśmy pewne zasady, ale nie wygląda na to, żeby to było przyczyną problemu. To był tylko ruch wewnętrzny do naszych laboratoriów. Dane nadal są przesyłane i nie jestem pewien, czy kontroluje to zapora sieciowa". Czas mijał, a ludzie próbowali zrozumieć, co się dzieje. Wendell podejrzewał, że zaczęło się to wczoraj wieczorem podczas prac konserwacyjnych, ale nie był pewien. "Hej!" Cezar prawie krzyknął. „Ruch został wstrzymany". Uśmiechnął się. „Ktoś coś naprawił lub zepsuł". Mike podniósł wzrok. "Co zrobiłeś?" Po sali rozległ się potok słów. Belinda skrzywiła się. – Cóż, nic nie zrobiłem. Jacob rozmawiał przez telefon komórkowy z klientem i uniósł brwi. „Wygląda na to, że wszystko działa dobrze. Z ich strony wygląda to normalnie. Daniel westchnął. „W porządku, możemy już iść do domu?" Zaczęła grać głośna muzyka, zagłuszając rozmowę. „Och, spójrz, Kiron dzwoni". Wendell odpowiedział. "Cześć, stary. Pić małymi łykami? Dziękuję, że oddzwoniłeś. Mieliśmy poważny problem i potrzebowaliśmy twojej pomocy, ale myślę, że tutaj wszystko jest pod kontrolą. „To dobrze" – powiedział Kiron, chichocząc ponad rozmowami w tle ruchliwej konferencji. „Mam tylko kilka minut. Jestem w trakcie hackatonu. Rzeczy są tu brutalne… – Wendell? Wendell otrząsnął się z zamyślenia. Rozejrzał się po sali konferencyjnej, po swoich kolegach. Mike pochylił głowę. „Czy masz coś jeszcze do dodania?" Wendell nie był pewien, jakie było pytanie. Nie zwracał na to większej uwagi, odkąd Mike wspomniał o śledztwie. Mózg Wendella odtwarzał przebieg ostatnich kilku miesięcy. To z pewnością było jego najciekawsze i najbardziej stresujące miejsce pracy jak dotąd. – Nie – wymamrotał. Dość stresujące. „Mam kolejne spotkanie" – powiedział Cezar. „Więc muszę biec." Mike odłączył laptopa od projektora. „OK, chłopaki; proszę, nie mów o tym, dopóki lepiej nie zrozumiemy, co się stało. Nie uruchamiajmy pociągu z plotkami. Atmosfera w pomieszczeniu była napięta. Ludzie się martwili, ale z raportu Mike'a wynikało, że zarząd chciał, żeby ktoś był winny. Oczywiście. Wendell miał złe przeczucie, że to będzie on. – Wendell – zawołał ponownie Mike. „Czy możesz zostać w pokoju, proszę?" Zaczynamy, pomyślał Wendell.

Znajomość sytuacji awaryjnych

Sytuacje awaryjne zdarzają się cały czas, w każdym aspekcie życia. Tym, co łączy te różne przypadki, jest to, że wywołują u ludzi ten sam rodzaj reakcji behawioralnej: wydobywają z nas to, co najlepsze i najgorsze. Świat IT stwarza dość specyficzny scenariusz. Z jednej strony jest to czysty, sterylny, uporządkowany i osłonięty świat, w którym ludzie pracują we względnym komforcie i bez niebezpieczeństwa fizycznego. Z drugiej strony czasami podejmują niemalże kapryśne decyzje o dalekosiężnych konsekwencjach. Charakter pracy IT nie zawsze odzwierciedla konsekwencje błędów i

wpadek, dlatego też sytuacje awaryjne, gdy do nich dochodzi, często rozwijają się w sposób nieprzewidywalny, obejmujący cały szereg kwestii etycznych. Dla strażaków próbujących ratować ludzi z płonącego budynku lub pracowników platformy wiertniczej na morzu sytuacje awaryjne często mają jasne i jednoznaczne znaczenie. Prawdziwa natura bestii nie zawsze jest widoczna, jeśli chodzi o serwery, bazy danych, a może urządzenia sieciowe. Dlatego nieetyczne zachowanie w sytuacjach awaryjnych w IT jest powszechne, oczekiwane i nieproporcjonalne do rzeczywistego zdarzenia. Wszystko sprowadza się do natury człowieka. Ogólnie rzecz biorąc, mamy tendencję do przeceniania zagrożeń o niskim prawdopodobieństwie i bagatelizowania tych o wysokim prawdopodobieństwie. Ludzie bardziej martwią się stopieniem reaktora jądrowego niż poślizgiem pod prysznicem. Utrata 100 GB danych nie jest tak realna, jak atak rekina. Stronniczość potwierdzenia również odgrywa swoją rolę. Połączenie tych dwóch elementów powoduje, że ludzie są mniej skłonni do dostrzegania problemów prowadzących do sytuacji awaryjnych i wydłużają okres odmowy akceptacji rozwijających się warunków sytuacji awaryjnych. Sytuacja nadzwyczajna to odejście od ustalonego, kontrolowanego stanu rzeczy, często określanego przez ramy polityk i zasad. Jednak każdą pracę IT odbiegającą od znanych warunków można uznać za odstępstwo, choć nie wszystkie takie sytuacje kończą się sytuacją awaryjną. Aby błąd przerodził się w awarię, muszą zaistnieć dwa inne czynniki: Czas – jeśli masz wystarczająco dużo czasu, aby zareagować na rozwijającą się sytuację, sformułować plan i złagodzić problem, może to być incydent, ale będzie nie być nagłym przypadkiem. Zazwyczaj sytuacje awaryjne wymagają, aby warunki pogarszały się szybciej, niż systemy i ludzie są w stanie je naprawić. Nieznany wynik – sytuacje awaryjne wymagają również, aby zaistniała sytuacja nie była wcześniej obserwowana ani dokumentowana oraz że nie są znane żadne rozwiązania ani środki zaradcze. Jeżeli taki przypadek istnieje, incydent można określić jako poważny lub nawet katastrofalny, ale wymaga on jedynie zastosowania znanych procedur w celu jego zakończenia lub złagodzenia. Sytuacje awaryjne wymagają zmiany parametrów problemu z nieznanych na znane, zanim będą mogły zostać rozwiązane.

Przygotuj się na nieoczekiwane

Prawie każdy inżynier, administrator systemu i technik w trakcie swojej kariery niewątpliwie znajdzie się w sytuacji awaryjnej. I prawie bez wyjątku takie sytuacje będą chaotyczne, a ludzie będą próbowali rozwiązać problemy bez pełnego zrozumienia zarówno symptomów, jak i konsekwencji swoich działań. Spowoduje to, że ludzie będą lekceważyć, ignorować lub omijać zasady i procedury, próbując szybko rozwiązać sytuacje kryzysowe. To żyzny grunt dla nieetycznych naruszeń. Może to brzmieć jak paradoks, ale etyczne podejście do radzenia sobie w sytuacjach awaryjnych polega na oczekiwaniu nieoczekiwanego. Brzmi to jak banał, ale wiąże się z koncepcją projektowania uwzględniającą porażkę, którą omawialiśmy w poprzednim rozdziale. Niemożliwe jest przewidzenie, zmapowanie lub poznanie wszystkich warunków, w których system może zawieść. Dlatego niemożliwe jest utworzenie reguł monitorowania lub środków łagodzących, które wyłapią każdą awarię. Rzeczywiście jest to kosztowny i nieskuteczny sposób prób powstrzymania chaosu i zapobiegania sytuacjom awaryjnym. Zamiast tego alternatywnym i etycznym podejściem powinno być zaakceptowanie i uwzględnienie możliwości, że systemy zawiodą, a ludzie popełnią błędy. Następnie, mając świadomość, że wynik będzie znany (porażka) spowodowany nieznanymi lub częściowo znanymi warunkami, można stworzyć scenariusze uwzględniające różne ewentualności i pozwalające na kontrolowaną reakcję na wynik. Koncepcja ta znana jest jako procedura rozbijania szkła.

Stłuc szkło

Sytuacje nadzwyczajne to delikatne sytuacje, często bez precedensu. W tym celu należy stworzyć formułę, która będzie miała zastosowanie we wszystkich sytuacjach awaryjnych. Formuła ta musi obejmować możliwie najszerszy zakres scenariuszy, wyników i reakcji ludzi na szybko rozwijające się sytuacje. Rzeczywiście, istnienie procedury „tłuczenia szyby” nie tylko wyjaśnia rodzaj działań, jakie

inżynierowie i administratorzy systemów powinni podjąć w sytuacji awaryjnej, ale zapewnia także chwilę wytchnienia, a raczej przestrzeń do myślenia, pozwalającą ludziom działać w skoordynowany, kontrolowany sposób. Eliminuje to lub przynajmniej ogranicza element czasowy, który jest dominujący w sytuacjach awaryjnych. Co najważniejsze, Break Glass minimalizuje możliwość nieetycznego zachowania i dalszych błędów w konsekwencji sytuacji awaryjnej. Definiuje, co należy zrobić w sytuacji awaryjnej w oparciu o stan awarii. Przyczyny tego stanu nie będą od razu zrozumiałe – jeśli tak jest, nie powinien to być nagły przypadek. Odpowiedź musi być jasno określona – prosta, skuteczna i zawsze aktualna. Definiuje komunikację w sytuacjach awaryjnych – element krytyczny, a często pomijany. Możliwe jest jednak, że pomimo najlepszych intencji i przygotowań, nadal będziesz musiał stawić czoła trudnej, nieznanej sytuacji, która może lub będzie wymagać naruszeń zasad etycznych. W tym przypadku będzie to wybór mniejszego zła – świadomie wybierzesz mniejsze naruszenie zamiast większego.

Powiedz wszystkim

Dla wielu osób naturalną reakcją na trudne sytuacje, zwłaszcza kryzysowe i awaryjne, jest postawa obronna. Z punktu widzenia IT oznacza to wahanie, niezdecydowanie i brak komunikacji. Nikt nie chce dzwonić do swojego menedżera o 2:00 w nocy i mówić mu, że jest problem. Co więcej, nikt nie chce dzwonić do swojego przełożonego i przyznać, że to on spowodował problem. Jednak komunikacja, niezależnie od tego, jak trudna może być, jest niezbędna w rozwiązywaniu sytuacji kryzysowych i ograniczaniu naruszeń etycznych. Pozwala innym ludziom zrozumieć sytuację i odpowiednio zareagować. Klienci mogą podjąć kroki, aby zminimalizować lub zapobiec utracie danych i finansów. Inne zespoły IT mogą pomóc w analizie i rozwiązaniu problemu, który doprowadził do sytuacji awaryjnej. Dobrze skoordynowana reakcja gwarantuje, że problem zostanie rozwiązany w najlepszy możliwy sposób. Sygnalizuje poziom odpowiedzialności i osobistej odpowiedzialności w imieniu zaangażowanych osób, w tym osób, które mogły być w pierwszej kolejności odpowiedzialne za spowodowanie sytuacji awaryjnej. Ukrywanie lub bagatelizowanie sytuacji awaryjnych jest często znacznie gorsze niż pierwotny problem.

Komunikacja zaczyna się od wewnątrz

„No cóż, potrzebujemy hasła. Pójdę po Mike'a.

Dobrym sposobem na ustanowienie kanału komunikacji na pierwszym poziomie jest eskalacja problemu do kierownictwa. Podczas gdy personel techniczny jest zajęty rozwiązywaniem problemu, menedżer może spróbować uzyskać szerszą wiedzę na temat problemu, koordynować pracę zespołów i podejmować niezbędne decyzje, zwłaszcza jeśli konieczne jest złamanie zasad. "Jasne. Popracuję nad przywróceniem kopii zapasowych z ostatniej nocy. Nie potrzebuję do tego żadnego hasła. Belinda stosuje standardowe procedury bez konieczności tłuczenia szkła. Informuje także swoich kolegów o tym, co zamierza zrobić. Co więcej, procedura tworzenia kopii zapasowej jest najprawdopodobniej dobrze udokumentowana i zarejestrowana, ponieważ stanowi część standardowej pracy operacyjnej, a zatem zapewnia również niezbędny ślad dla wszelkich dochodzeń lub analiz po zdarzeniu. „Połowa reguł zapory sieciowej jest złamana” – mruknął Alex. „Mam zamiar je usunąć”. Alex mówi pomieszczeniu, co robi. Byłoby jeszcze lepiej, gdyby ktoś robił notatki z działań na osi czasu, korzystając z udostępnionego dokumentu, aplikacji do czatu lub podobnego rozwiązania. „Czy nie powinniśmy skorzystać z zarządzania konfiguracją?” Pytanie Wendella podkreśla kilka dobrych punktów. Po pierwsze, jest skłonny rzucić wyzwanie pracy w sytuacjach awaryjnych (nie jest to bezpłatne zaproszenie do zrobienia czegokolwiek). Co więcej, czyni to w sposób zgodny z przykazaniem. Zakładając, że zarządzanie konfiguracją jest skonfigurowane w ramach kontroli wersji, a tak powinno być, zmiany będą śledzone i będzie można je przeglądać w razie potrzeby. „OK, chłopaki, musimy to

powstrzymać. Rozwiążemy problem później. Na razie musimy zatrzymać ruch sieciowy". Mike próbuje zapewnić sobie pewien poziom kontroli nad sytuacją. Próbuje ująć problem w ramy i określić pożądany rezultat oraz kolejność działań. Co więcej, ogranicza również zakres procedury Break Glass. Pozwala to na szybszy powrót do normalnej pracy po zdarzeniu. „Więc niech lepiej się upewni, że nas nie rozłączy… Po prostu zatrzymajmy bazę danych, a ja rozpocznę przywracanie". Musi istnieć skuteczna komunikacja pomiędzy członkami zespołu. Opowiedzenie wszystkim o zamierzonej pracy i konsekwencjach minimalizuje ryzyko dalszych uszkodzeń lub powikłań. Na przykład, jeśli sieć Alexa zostanie przez pomyłkę odłączona, uniemożliwi mu to udzielenie pomocy w sytuacji awaryjnej, a nawet może pogorszyć sytuację.

Nie mówienie powoduje więcej pracy

„Och, zespół sieciowy zaczął używać portfela haseł. Mike, ta lista jest nieaktualna.

Chociaż istnienie portfela haseł jest dobrą praktyką w zakresie bezpieczeństwa, Mike nie był świadomy, że używane jest nowe narzędzie. Co więcej, istniejąca lista jest nieaktualna, co stanowi naruszenie zasad, w jaki należy utrzymać procedury dotyczące stłuczenia szkła. Oznacza to, że procedury Break Glass oferują sprzeczne informacje tym, którzy ich potrzebują, i będą miały dwa różne wyniki, w zależności od tego, która lista zostanie przejrzana.

„Hm. Wygląda na to, że Gopal także pracuje nad DB01. Wcześniej dokonał aktualizacji. Może kończy konfigurację. Gopal, jesteś jeszcze na moście? Gopala?"

Wygląda na to, że wprowadzono zmiany, które nie zostały udokumentowane ani udostępnione reszcie zespołu. Co więcej, Gopal nie komunikował swojej pracy, co pogorszyło sytuację. Dalsze działania mogą faktycznie skomplikować sprawę, gdyż członkowie zespołu Gopala mogą działać w oparciu o błędne założenia.

Zostaw ślad

Zarówno w codziennych sytuacjach, jak i w sytuacjach awaryjnych, komunikacja pozostaje istotnym, niezbędnym ogniwem łączącym różne elementy układanki: ludzi, maszyny i problemy pomiędzy nimi. W sytuacjach awaryjnych nabiera to jeszcze większego znaczenia, ponieważ sytuacje awaryjne są zazwyczaj nieudokumentowanymi, pierwszymi przypadkami nieznanych scenariuszy i problemów. Zapewnienie dowodów umożliwiających analizę pełnej sekwencji zdarzeń jest niezwykle istotne, zwłaszcza po rozwiązaniu sytuacji awaryjnej, gdy ludzie mają wystarczająco dużo czasu i swobody, aby szczegółowo rozwiązać problemy. Co więcej, kryminalistyczny ślad danych zapewnia przejrzystość i jasność działań i objawów oraz umożliwia przywrócenie normalnego funkcjonowania po zakończeniu sytuacji awaryjnej. W scenariuszach Break Glass zostaną naruszone standardowe procedury i mogą nastąpić destrukcyjne działania, które zmienią oczekiwany stan narzędzi i systemów. Jeśli nie ma śladu, w jaki sposób zostały one zmienione, rozróżnienie pomiędzy pierwotnym problemem a awarią może nie być możliwe (co również utrudnia analizę sytuacji awaryjnej), a przywrócenie systemów może zająć znacznie więcej czasu w pożądany stan. Zbieranie informacji podczas pracy nad pilnymi sprawami może być trudne, ale należy to zrobić. Być może pełne dzienniki i monitorowanie nie będą dostępne, ale nadal możliwe jest śledzenie śladów w postaci e-maili, wiadomości na czacie, list na tablicy, a nawet długopisu i papieru.

Użyj narzędzi do rejestrowania

„Och, zespół sieciowy zaczął używać portfela haseł".

Portfel haseł to narzędzie rejestrujące dostęp, dzięki czemu zapewnia ślad do hasła Break Glass.

„Zapisz, komu przekazujesz każde hasło.”

Może to nie jest idealne rozwiązanie, ale lepsze niż brak jakichkolwiek informacji na temat użycia hasła. Dziennik papierowy jest rozsądną alternatywą, gdy ścieżka elektroniczna nie jest dostępna. Wrócił i zaczął ciąć kopie na paski, tak aby na każdym pasku było tylko jedno hasło… „Daj mi je, ja je zniszczę, żeby nie trzeba było ich później zmieniać”. Po raz kolejny zachowanie Wendella nie jest idealne, ale przynajmniej stara się ograniczyć dostęp do poszczególnych haseł. Podobnie sugestia Jakuba zmniejszy rozmiar szlaku. Dzięki temu można rozbić szkło bez naruszania pozostałych przykazań. Co więcej, co do zasady hasła należy zmieniać w przypadku sytuacji awaryjnej lub naruszenia, a Jacob powinien zaplanować tę czynność po zakończeniu zdarzenia.

„Narzędzie do zarządzania konfiguracją nadpisało Twoją zmianę.”

Pomimo sytuacji awaryjnej Break Glass nie pozwala na ręczne zmiany konfiguracji systemu. Ogólnie rzecz biorąc, podczas obsługi sytuacji awaryjnych mogą być wymagane pewne zmiany w normalnych procedurach, ale należy je ograniczyć do minimum, a administratorzy systemów i inżynierowie powinni w miarę możliwości przestrzegać standardowych wytycznych pracy.

Nie trać kontroli – Proszę bardzo, Wendell.

Chociaż pomoc Mike'a jest doceniana, sposób, w jaki obchodził się z hasłami, jest niewłaściwy z etycznego punktu widzenia. Mike ujawnił hasła bez wyraźnej potrzeby ich poznania i bez rejestrowania transakcji. Mike mógł zdecydować, kto spośród członków zespołu powinien zajmować się uprzywilejowanym dostępem haseł do różnych narzędzi zarządzania i udostępniać im jedynie dane uwierzytelniające.

„Hasło do portfela zostało zapisane na dole zadrukowanej kartki, którą Kiron trzyma pod klawiaturą”.

Stereotypy i klisze istnieją nie bez powodu. Są głęboko zakorzenione w złych praktykach. Trzymanie haseł na kartce pod klawiaturą brzmi jak szkic z serialu komediowego, ale ogólnie jest to zła praktyka. Nie pozostawia śladów tego, kto użył hasła, poza oczywistym, rażącym zagrożeniem bezpieczeństwa.

„… gorączkowo zapisywał hasła uprawnień dla różnych typów systemów.”

Zachowanie Mike'a nie zapewnia cyfrowego dziennika tego, kto otrzymuje hasło. Po rozwiązaniu sytuacji awaryjnej nie będzie żadnych dowodów użycia (lub niewłaściwego użycia) ani możliwości unieważnienia danych uwierzytelniających. Oznacza to, że zespoły będą musiały zmieniać swoje hasła, jeśli chcą zachować odpowiedni poziom kontroli dostępu.

„Po prostu daj mi całą listę” – powiedział spokojnie Henry. „Będę potrzebował kilku z nich do maszyn wirtualnych i systemów laboratoryjnych”.

Nie ma sposobu, aby sprawdzić, jakiego hasła będzie używał Henry. To z kolei oznacza, że nie ma możliwości sprawdzenia podjętych przez niego kroków, ponieważ robi wiele rzeczy na raz. Jeśli w wyniku sytuacji awaryjnej wystąpią komplikacje, prawie niemożliwe będzie zrozumienie, kto miał dostęp do różnych systemów i czy w jakiś sposób te działania pogorszyły pierwotny problem. Może to być szczególnie trudne w przypadku wycieków i naruszeń danych, gdzie kluczowa jest możliwość oddzielenia złośliwego dostępu z zewnątrz od rutynowej pracy w systemach.

„Myślę, że użyję do tego hasła konsoli lokalnej.”

Korzystanie z konsoli lokalnej omija wszelkie narzędzia śledzące dostęp do plików lub działania uprzywilejowanych użytkowników. Podobnie jak sugestia Henry’ego, sprawi to, że analiza legalnych i potencjalnie złośliwych działań podczas sytuacji awaryjnej będzie prawie niemożliwa. Procedury Break

Glass powinny obejmować bezpośredni dostęp do serwerów w centrach danych w sposób pozwalający na pozostawienie śladu i umożliwienie późniejszej analizy kryminalistycznej.

"Nie ma na to czasu. Po prostu zrobię to ręcznie.

Pominięcie zarządzania konfiguracją oznacza, że nie będzie dziennika zmian Alexa. Uniemożliwi to rozróżnienie pomiędzy pomyłkami, błędami, przestarzałymi przepisami, a jego pracą ręczną w sytuacji awaryjnej.

"Co to za różnica?" Cezar sprzeciwił się. „I tak będziemy przywracać."

Podejście Cezara nie sprzyja rozwiązaniu sytuacji. Bez dziennika działań i pełnego zrozumienia tego, co się dzieje, ten sam problem z pewnością powtórzy się w przyszłości. Im mniej dowodów na istnienie problemu po incydencie, tym trudniej będzie zespołom administrującym systemem rozwiązać problem i zrozumieć warunki, które doprowadziły do sytuacji awaryjnej, co uniemożliwia im opracowanie skutecznego rozwiązania.

"Co zrobiłeś?"

Działania muszą być oczywiste i przejrzyste. Członkowie zespołu nie powinni zadawać sobie nawzajem pytań, aby zrozumieć, co zostało zrobione. Szczegółowy, precyzyjny dziennik techniczny powinien dostarczyć niezbędnych odpowiedzi. „W porządku, możemy już iść do domu?"

Takiego nastawienia można się spodziewać pod koniec długiego, frustrującego dnia. Trudno winić ludzi, którzy chcą po prostu uciec. Jednakże zespół powinien przed wyjazdem upewnić się, że wszystko jest dobrze udokumentowane i uporządkowane. Oszczędzi im to bólów głowy i wyczerpujących sytuacji awaryjnych w przyszłości.

Idealny scenariusz dla stłuczonego szkła

Jeśli pomyślimy o idealnym scenariuszu, prosta odpowiedź brzmi: nie może być takiego. Nie da się stworzyć niezawodnego środowiska IT, w którym nic nigdy nie będzie się psuć. W najlepszym przypadku będzie to konfiguracja, która skutecznie i stale minimalizuje ryzyko dzięki inteligentnym praktykom, wysokiemu poziomowi wykonania, dokładnym systemom monitorowania oraz solidnym narzędziom do tworzenia kopii zapasowych i odzyskiwania danych.

Niepowodzenie się wydarzy

Najważniejsze jest uznanie istnienia awarii, uwzględnienie ich w architekturze i projektowaniu środowiska IT, a następnie odwzorowanie ich na trwające procedury operacyjne. Awarie należy klasyfikować na podstawie dwóch głównych kryteriów: prawdopodobieństwa ich wystąpienia (niskie/wysokie) oraz poziomu szkód, jakie spowodują (niskie/wysokie). Połączenie tych dwóch wartości określi ryzyko i koszt, jaki mogą ponieść sytuacje awaryjne, a co za tym idzie, koszt działań łagodzących i przywrócenia działania w przypadku wystąpienia sytuacji awaryjnych. Mapowanie ryzyka (podobnie jak zarządzanie zmianą) pozwala na wdrożenie odpowiednich mechanizmów. Skrajnymi przykładami są inne sektory przemysłu, takie jak energia atomowa i ruch kolejowy. Prawdopodobieństwo awarii elektrowni jądrowej jest niezwykle niskie, ale ze względu na ogromny potencjał trwałych zniszczeń i wpływu na życie ludzkie, reaktory jądrowe są wyposażone w liczne systemy redundancji zaprojektowane w celu zapobiegania awariom. Z drugiej strony awarie pociągów są dość częste, ale ryzyko jest zazwyczaj niskie – ludzie spóźniają się do pracy, występują zakłócenia w ruchu, ale szkody są często minimalne. Dlatego można dopuścić do awarii pociągów. Natomiast zarządzanie ruchem pociągów to już zupełnie odrębna kwestia, która ze względu na ryzyko życia

uwzględnia liczne rozwiązania łagodzące (automatyczne hamowanie, szlabany na przejazdach kolejowych itp.).

Być przygotowanym

Procedura Break Glass wypełnia lukę w przypadku awarii systemu. Powód tego jest prosty: nie można odwzorować każdego możliwego scenariusza i czasami trzeba polegać na procedurach Break Glass. Jeżeli zaistnieje ewentualność, która nie została przewidziana, zaplanowana i uwzględniona w procedurze, jest ona niekompletna, a to oznacza, że pewnego dnia może nastąpić sytuacja awaryjna, która przekształci się w sytuację rozbicia szyby, na którą nie będzie natychmiastowe rozwiązanie. W związku z tym procedury stłuczenia szyby można uznać za rozwiązanie „ostateczności". Niekoniecznie będą mieli konkretne odpowiedzi, ale ustalą sekwencję działań, które powinny pomóc rozwiązać nieznany stan i przywrócić sytuację do normalnego funkcjonowania. Wróćmy do naruszenia, którym zajęli się Wendell i jego współpracownicy. Nie wiedzieli (i nadal nie wiedzą), w jaki sposób doszło do naruszenia i jakie sekwencje błędów, błędów lub błędów oprogramowania do niego doprowadziły. Ale to zupełnie w porządku, ponieważ ideą procedur Break Glass nie jest dogłębne rozwiązywanie problemów z systemami i zrozumienie wszystkiego. Daleko stąd. Chodzi o to, aby jak najszybciej przywrócić normalny, kontrolowany stan. W szczególności scenariusz wymaga tylko

• Zrozumienie, że następuje niekontrolowane wykorzystanie danych (szczegóły nie są ważne)

• Istnienie dobrze określonej procedury wyjaśniającej, co należy zrobić w takiej sytuacji, na przykład:

• Odczekaj 30 minut na analizę.

• Zakończ łączność sieciową, usuwając fizyczny dostęp kablowy.

• Wykonaj przywracanie systemu.

Oznacza to, że zespół Mike'a nie musi być ekspertem w dziedzinie hakowania, ponieważ w zaporze sieciowej lub oprogramowaniu przełącznika sieciowego, w bazie danych, w aplikacji klienta, w błędnie skonfigurowanych regułach może znajdować się nieskończona liczba luk w zabezpieczeniach. Powinni mieć udokumentowaną procedurę, która obejmuje

• Wykrywanie wyjścia danych

• Podstawowy zestaw analiz umożliwiający, jeśli to możliwe, niezakłócającą naprawę

• Dobrze odwzorowany zarys łączności z centrum danych, umożliwiający technikom dostęp do serwera, którego dotyczy problem, i jego odłączenie (opcjonalne może być również rozwiązanie oparte na oprogramowaniu)

• Dobrze zaprojektowana i przetestowana procedura, która umożliwia naprawę systemu lub przywrócenie go do nieskazitelnego stanu przy minimalnej utracie danych lub funkcjonalności

Ostatecznie procedury Break Glass to kombinacja kroków, które można wykonać szybko, aby złagodzić dalsze szkody, nawet jeśli pełny stan problemu nie jest dobrze poznany. Zamiast grzęznąć w bezczynności, wahaniu i zamieszaniu, administratorzy systemów będą mieli jasne ramy tego, co robić, nawet jeśli będą mieli jedynie częściowy wgląd i kontrolę nad pierwotną przyczyną sytuacji awaryjnej.

Trzymaj to razem

Rzeczywiście, sytuacje awaryjne nie są definiowane tylko przez utratę kontroli nad systemami i pilność czasu, ale często wiążą się z błędną komunikacją i brakiem koordynacji. Zorganizowanie skutecznej pracy w sytuacjach awaryjnych może być trudne, ponieważ ludzie rzadko szkolą się w tym zakresie, a

wielu nie reaguje dobrze w sytuacjach stresowych. Oto kilka rzeczy, o których warto pamiętać, jeśli znajdziesz się w sytuacji awaryjnej związanej z komputerem:

• Pierwszą kolejnością rzeczy jest faktyczne określenie sytuacji w taki sposób, aby można było sformułować opis problemu. Jeśli nie ma jasnej definicji tego, co jest nie tak, nie ma skutecznego rozwiązania. Nie oznacza to, że pierwotna przyczyna jest już jasna, ale objawy są dobrze poznane.

• Powinien być ktoś odpowiedzialny – niektóre firmy mogą mieć wydzieloną funkcję menedżera ds. incydentów, która może również przejąć taką odpowiedzialność w sytuacjach awaryjnych. Może to być jednak dowolna osoba, o ile rozumie wymagania związane z jej (tymczasową) rolą.

• Komunikacja jest niezbędna w budowaniu niezbędnej świadomości sytuacyjnej, upewnianiu się, że ludzie nie działają wbrew sobie i ułatwianiu szybszego rozwiązania.

Prace awaryjne należy wcześniej ustalić. Brzmi to jak scenariusz z paragrafem 22. Jeśli opis problemu jest znany z góry, należy go złagodzić i w rezultacie nigdy nie powinno dojść do sytuacji awaryjnej. Z drugiej strony, jeśli problem jest nieznany, jak można z góry określić pracę? Rzeczywiście, nie da się przewidzieć niektórych niepowodzeń ani łańcucha zdarzeń, który po nich nastąpi, ale całkowicie możliwe jest posiadanie awaryjnego planu działania nawet w przypadku nieznanych sytuacji. Chociaż konkretne zadania będą się różnić w zależności od scenariusza, ogólna koncepcja pozostaje taka sama. To prawie jak przepis na to, co zrobisz, jeśli zgubisz się w dużym mieście. Układ ulic będzie inny w Medellin i Montrealu, ale podstawowa idea pytania o drogę, korzystania z mapy lub kontaktowania się z policją jest uniwersalna. Z planu awaryjnego należy skorzystać, gdy stanie się jasne, że nie ma znanego rozwiązania sytuacji awaryjnej w danym zakresie i czasie lub że ryzyko i szkody są zbyt duże, aby sytuacja awaryjna mogła być kontynuowana – to Break Glass w ramach Break Glass.

Pokaż człowiekowi, jak rozwiązywać problemy IT, a odpocznie przez jeden dzień; naucz człowieka rozwiązywać problemy informatyczne, a będzie zajęty do końca życia. Ogólne wytyczne dotyczące sytuacji awaryjnych powinny być następujące:

• Instrukcje muszą być dokładne i aktualne.

• Instrukcje muszą być proste – czas będzie odgrywał kluczową rolę, a ludzie nie powinni na bieżąco odkrywać, jak postępować w sytuacjach awaryjnych.

• Należy ćwiczyć sytuacje awaryjne – ponownie nie da się zaplanować wszystkiego, ale można przetestować scenariusze wysokiego ryzyka. Regularne, okresowe ćwiczenia symulacyjne w sytuacjach awaryjnych mogą zaszczepić pewien poziom znajomości systemów i procedur. Zazwyczaj będzie to część szerszej, strategicznej polityki zwanej odzyskiwaniem po awarii (DR). Będzie dotyczyć katastrofalnych awarii znaczących części infrastruktury IT i postępowania wokół niej, z naciskiem na jak najszybsze przywrócenie funkcjonalności i produktywności. Działania związane z DR mogą obejmować przywracanie danych, uruchamianie zewnętrznego centrum danych, aktywację usług infrastrukturalnych, ponowną instalację krytycznych aplikacji i podobne kroki, które mogą być potrzebne do utrzymania działania firmy.

Historia z okopów IT: co 3 miesiące przeprowadzaliśmy test DR, a szczegółowe informacje były znane tylko niewielkiej liczbie osób, np. kluczowej osobie kontaktowej z klientem, menedżerowi centrum danych i kilku szefom zespołów inżynieryjnych. Nie informując o tym całodobowego NOC, obniżylibyśmy od 10 do 25% środowiska obliczeniowego. Następnie powiadamiali kierownika ds. incydentów (który miał dostęp do najdrobniejszych szczegółów symulacji), który następnie zbierał różne zespoły w celu rozwiązania problemu, uruchomienia zdalnej lokalizacji w trybie online, a następnie przywrócenia normalnej produktywności. Za każdym razem wyciągaliśmy mnóstwo cennych

lekcji. Zawsze będzie kilkanaście drobnych rzeczy, które pójdą nie tak, od nieaktualnych list telefonów, przez brakujące zasady monitorowania, po problemy z zarządzaniem aktywami. Za każdym razem czuliśmy się nieco lepiej, ale pokazało nam to, że w prawdziwej sytuacji awaryjnej nie poradzimy sobie zbyt dobrze i że ciągłe testowanie było niezbędne. To było niezwykle cenne ćwiczenie.

Szlak Informacyjny

• Sytuacje awaryjne to doskonała okazja, aby sprawy prześlizgnęły się przez szczeliny. Ludzie mogą zakładać, że skoro sprawy już się skomplikowały, mogą porzucić ostrożność. Niestety, stwarza to dalsze problemy na dalszej drodze.

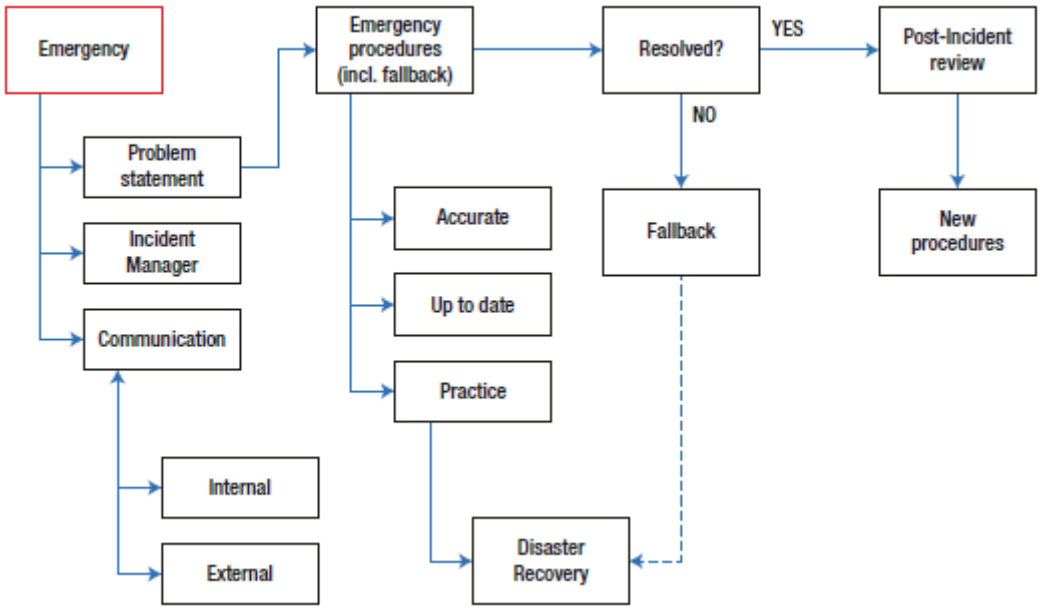
• Ważne jest, aby pozostawić ślad wykonanej pracy i zachować otwarte kanały komunikacji. W pewnym sensie sytuacje kryzysowe wynikają z nieoczekiwanych zmian w środowisku, których harmonogram jest napięty i których skutki są nieznane. Komunikacja powinna odbywać się przy użyciu najlepszego do tego narzędzia narzędzia – narzędzia do przesyłania wiadomości w czasie rzeczywistym umożliwiającego natychmiastową komunikację oraz poczty elektronicznej w celu okresowych aktualizacji. Telefony są przydatne, ponieważ ludzie zazwyczaj mogą rozmawiać szybciej i przekazywać wiadomości skuteczniej niż na piśmie, ale rozmowy telefoniczne rzadko pozostawiają ślad i łatwo jest źle zrozumieć informacje techniczne.

• Jeśli masz zamiar celowo dopuścić się etycznego naruszenia ustalonych procedur, dokładnie to udokumentuj.

• Sprawdzaj każdy krok – szybka praca może stwarzać wrażenie pilności, ale zmiany wprowadzane w pośpiechu mogą być równie niebezpieczne i ryzykowne jak pierwotna sytuacja awaryjna.

• Przegląd po incydencie – po zakończeniu sytuacji awaryjnej, przy pełnym zrozumieniu pierwotnej przyczyny, objawów, wyniku i środków zaradczych podjętych w celu rozwiązania problemu, należy przeprowadzić przegląd, który szczegółowo wyszczególni wnioski wyciągnięte z incydentu. Pozwala to na analizę przyczyn awarii, a także wszelkich niezamierzonych konsekwencji, które wystąpiły w wyniku scenariusza Tłuczenia Szyby. Ten krok jest niezbędny, aby zapobiec konieczności rozbicia szyby następnym razem.

Skuteczna sekcja zwłok sytuacji awaryjnej przekształci się w przyszły zestaw zasad i procedur. Ogólny przepływ w sytuacji awaryjnej pokazano na rysunku



Proś o przebaczenie

Wszyscy popełniają błędy. Sposób, w jaki ludzie sobie z nimi radzą – zarówno swoimi, jak i tymi stworzonymi przez innych – definiuje etyczne podłoże całego środowiska IT. W dłuższej perspektywie takie podejście będzie miało wpływ na poziom innowacyjności i ryzyka, jakie ludzie będą skłonni podjąć w ramach swojej pracy. Jeśli popełniłeś błąd w swojej pracy, powinieneś „przyznać się". Nie ma to na celu poniżania ani karania. Powinien to być akt introspekcji, który pozwala ludziom zrozumieć, gdzie popełnili błąd i jak uniknąć takich sytuacji w przyszłości. Podobnie powinieneś zaakceptować fakt, że Twoi współpracownicy czasami będą się mylić. Zdrowe miejsce pracy, w którym ludzie mogą omawiać swoje błędy i je poprawiać, zazwyczaj sprzyja wyższemu poziomowi innowacyjności i współpracy. Jeśli ludzie boją się zabrać głos, będą unikać wykonywania „ryzykownych" zadań, co może prowadzić do stagnacji intelektualnej. Co gorsza, ze strachu mogą próbować ukryć swoje wpadki, co znacznie utrudnia radzenie sobie w sytuacjach awaryjnych.

Sytuacje awaryjne i menedżerowie

Menedżerowie odgrywają kluczową rolę w sposobie, w jaki ich zespoły radzą sobie w sytuacjach awaryjnych. Często robią to źle. Naturalnie osoby, którym powierzono kierowanie zespołami lub grupami, założą, że posiadają umiejętności niezbędne do radzenia sobie w sytuacjach awaryjnych. Niestety, chociaż wielu menedżerów ma dobre umiejętności „czasu pokoju", mogą nie nadawać się najlepiej do sytuacji kryzysowych. Problemy techniczne mogą być często bardzo złożone i obejmować nieliniową interakcję pomiędzy różnymi komponentami. Objawy mogą być niejasne lub niejasne, a ich rozwiązanie będzie wymagało dużej wiedzy specjalistycznej, aby można było opanować sytuacje o nieznanym stanie. Menedżerowie liniowi niekoniecznie muszą posiadać odpowiednią wiedzę, aby w takich scenariuszach podejmować decyzje. Administratorzy systemów zajmujący się sytuacjami awaryjnymi będą już i tak mieli wystarczająco dużo stresu, bez kogoś, kto by ich nadzorował. Obecność menedżera może rozpraszać, a nawet przynosić skutki odwrotne do zamierzonych, szczególnie jeśli dana osoba nie ma odpowiednich umiejętności, aby w pełni zrozumieć problem. Frustracja w stosunku do menedżerów: gdy zdarzyła się sytuacja awaryjna, typową procedurą byłoby zebranie przez dyżurnego menedżera na ten tydzień grupy inżynierów, którzy najprawdopodobniej lub najbardziej nadają się do poradzenia sobie z sytuacją, wprowadzenie ich do pokoju i uruchomienie mostu telefonicznego – często z kontaktem z klientem po drugiej stronie – a następnie rozpocznij pracę nad

problemem. Zwykle problem nie byłby dobrze zdefiniowany, więc spędzaliśmy czas nawet próbując sformułować problem, zanim będziemy mogli faktycznie przeprowadzić wstępną analizę. Hałas dochodzący z mostka telefonicznego i liczne równoległe rozmowy były dość rozpraszające i utrudniały koncentrację na zadaniu. Menedżer dyżurny i czasami inni (w tym menedżerowie wyższego szczebla, którzy często dołączali do niego w miarę postępu lub eskalacji sytuacji) siedzieli z tyłu sali, pracując nad niepowiązanymi czynnościami na swoich laptopach, a następnie od czasu do czasu podnosili głowy i poproś o „aktualizację statusu". Rzadko koordynowali pracę, często nie mieli wiedzy technicznej ani przydatnych porad, a ich postawa sprawiała, że ludzie czuli się tak, jakby byli „monitorowani". Rzadko naprawiamy coś w ten sposób podczas sesji awaryjnych i wydawało mi się, że to zwykła czynność. W sytuacji awaryjnej działania menedżera powinny ograniczać się do koordynacji i komunikacji. Obejmuje to nadanie priorytetu sytuacji awaryjnej w stosunku do innych prac ekspertów technicznych oraz, jeśli to konieczne, planowanie zespołów zmianowych. Menedżer zarządzający sytuacją kryzysową powinien być jedyną osobą, od której wymaga się przekazywania statusu innym menedżerom. Gdy popiół ostygnie, menedżerowie powinni pielęgnować kulturę otwartego dialogu, bez obawy przed karą. Często to mściwa postawa liderów zespołów lub menedżerów powoduje, że ludzie „bunkrują się" w swojej pracy.

Wniosek

Sytuacje awaryjne wynikają z dwóch elementów – nieznanego wcześniej stanu awarii i, co jeszcze ważniejsze, braku przygotowania firm i zespołów technicznych na poradzenie sobie z takimi warunkami. Właściwym podejściem jest pewność, że wystąpią sytuacje awaryjne. W oparciu o doktrynę projektowania uwzględniającego awarię pomysł polega na włączeniu sytuacji awaryjnych do codziennych działań, a następnie przejściu od katastrofalnych scenariuszy „co by było, gdyby" do skutecznych i solidnych środków łagodzących. Te środki łagodzące są ujęte w procedurach Break Glass, które muszą być kompletne, aktualne, odpowiednie do ryzyka i prawdopodobieństwa scenariuszy, których dotyczą, oraz na tyle uniwersalne, aby można je było zastosować w najszerszym zakresie warunków. Procedury Break Glass obejmują również skuteczną komunikację i szczegółową ścieżkę informacyjną, dzięki czemu można ograniczyć naruszenia etyczne i niestandardowe działania w pracy w sytuacjach awaryjnych. Dzięki dokładnym danym administratorzy systemów mogą rozwiązywać nieznane wcześniej problemy i włączać je do codziennej pracy, tak aby ta sama awaria nigdy nie musiała się powtarzać. W tej historii poczesne miejsce zajmuje Mike, pełniący rolę menedżera ds. incydentów w sytuacji kryzysowej, przed którą stanął jego zespół. Rzeczywiście, przywódcy odgrywają kluczową rolę w szerszym zakresie.