Czytaj lub słuchaj artykuł online

Zeskanuj kod QR, aby otworzyć artykuł na XO.PL

Źródło artykułu:

https://xo.pl/it-na-wesolo-sec-basics

BEZPIECZEŃSTWO IT

Bezpieczeństwo IT, czyli dlaczego wszystko będzie dobrze to za mało

W dniu uroczystego otwarcia nowej siedziby Pana Kierownika pod budynkiem zebrała się prasa, komisja odbiorowa, firma ochroniarska i strażacy. Na fasadzie wisiał transparent: **CENTRUM BEZPIECZEŃSTWA ABSOLUTNEGO — 100% GWARANCJI!** Pan Kierownik zamierzał udowodnić, że jego firma jest odporna na włamania, wirusy, awarie, złodziei, pomyłki, a zapewne również na zdrowy rozsądek. Grzesiu przyjechał z teczką dokumentów i kanapką. Jedno z tych dwóch miało mu uratować dzień. 🤣

Wstęgę przetniemy, jak tylko otworzymy drzwi

— SZANOWNI PAŃSTWO! — rozpoczął Pan Kierownik. — OTWIERAMY BUDYNEK, DO KTÓREGO NIKT NIEPOWOŁANY NIE WEJDZIE!

— A powołany? — zapytał Grzesiu.

— POWOŁANY TEŻ NIE, JEŚLI NIE MA ZGODY!

— Czyjej?

— MOJEJ!

— A kto zatwierdzi pana wejście?

— PANIE GRZESIU, NIECH PAN NIE PSUJE KONFERENCJI PRASOWEJ PYTANIAMI!

W tym momencie z bocznego wejścia wyszła pani Agnieszka, księgowa.

— Panie Kierowniku, sześć osób utknęło w środku. System kontroli dostępu nie otwiera drzwi.

— DOSKONALE! CZYLI DZIAŁA!

— Nie otwiera ich również od środka.

— TO NIECH POCZEKAJĄ NA MOJĄ ZGODĘ!

— Panie Kierowniku — wtrącił przedstawiciel straży pożarnej — wyjścia ewakuacyjne nie mogą zależeć od pańskiej zgody.

— NAWET W MOIM BUDYNKU?!

— Zwłaszcza w pańskim.

Grzesiu odłożył kanapkę. — I to jest pierwszy problem z bezpieczeństwem. **Ochrona, która uniemożliwia normalne korzystanie z obiektu albo bezpieczną ewakuację, może sama stać się zagrożeniem.** W informatyce działa podobna zasada: zabezpieczenia mają chronić działalność, nie ją paraliżować.

Trzy filary, których kierownik nie zamawiał

Komisja weszła do sali konferencyjnej. Na ścianie wisiał schemat dwudziestu siedmiu systemów alarmowych.

— Wszystkie nasze dane są bezpieczne! — oznajmił Pan Kierownik.

— Czyli co dokładnie? — zapytała przewodnicząca komisji.

— NIKT ICH NIE UKRADNIE!

— A jeśli ktoś zmieni kwotę na fakturze z tysiąca na sto tysięcy? — spytała Agnieszka.

— ZABRONIONE!

— A jeśli nikt niczego nie ukradnie ani nie zmieni, ale nie będziemy mogli otworzyć systemu księgowego?

— TO GRZESIU NAPRAWI!

— A jeśli Grzesiu będzie na urlopie?

— PAN GRZESIU NIE MA URLOPU!

— Mam. Nawet sporo niewykorzystanego.

W ochronie informacji często mówi się o trzech filarach: **poufności, integralności i dostępności** (ang. *confidentiality, integrity, availability*, czyli CIA). **Poufność** ogranicza poznanie informacji przez nieuprawnione osoby. **Integralność** dotyczy ich poprawności oraz ochrony przed nieuprawnioną zmianą. **Dostępność** oznacza, że uprawnione osoby mogą korzystać z danych i usług wtedy, gdy ich potrzebują. Ochrona jednego filaru kosztem całkowitego zniszczenia pozostałych to zwykle zły interes.

— A JEŚLI WSZYSTKIE DOKUMENTY ZAMKNIEMY W SEJFIE I ZALEJEMY BETONEM?!

— Poufność może się poprawić — przyznał Grzesiu.

— HA! WIEDZIAŁEM!

— Dostępność spadnie jednak mniej więcej do poziomu wykopalisk archeologicznych.

— TO KUPIMY MŁOT PNEUMATYCZNY!

— Właśnie wynalazł pan odzyskiwanie danych metodą budowlaną.

Haker z teczką i bez kominiarki

Na odbiór zaproszono również audytora bezpieczeństwa. Miał przetestować procedury za zgodą firmy i w ustalonym zakresie. Nie przyniósł łomu ani laptopa z zielonymi literami. Przyniósł teczkę i identyfikator z napisem „SERWIS”.

— Dzień dobry, przyszedłem do klimatyzacji. Pan Kierownik kazał mnie natychmiast wpuścić.

— Poproszę o potwierdzenie zlecenia — odparła recepcjonistka.

— Ale on teraz prowadzi konferencję! Nie wolno mu przeszkadzać!

— W takim razie poczekamy.

— Zepsuje się klimatyzacja!

— To sprawdzimy zgłoszenie w systemie. Ma pan numer?

Audytor uśmiechnął się i pokazał dokument. — Gratuluję, test zaliczony. Sprawdzałem, czy powołanie się na autorytet kierownictwa wystarczy, by ominąć procedurę.

Wpadł Pan Kierownik.

— GDZIE JEST TEN HAKER?!

— Tutaj — powiedział Grzesiu. — Sami go zatrudniliśmy.

— TO DLACZEGO JESZCZE NICZEGO NIE UKRADŁ?!

— Bo test odbywa się legalnie, w uzgodnionych granicach.

— AHA. TO NIECH UKRADNIE COŚ NIEWAŻNEGO!

— Panie Kierowniku, w tym właśnie problem: dla złodzieja nie zawsze wiadomo z góry, co okaże się ważne.

Ataki nie zawsze zaczynają się od łamania szyfrów. Czasami ktoś próbuje nakłonić człowieka do ujawnienia informacji albo wykonania niewłaściwej czynności. To **socjotechnika**; jej popularną formą jest **phishing**. Dobra procedura sprawdza tożsamość i uprawnienia, zamiast polegać na pewnym głosie, pośpiechu albo słowach „szef kazał”.

Ryzyko ma własne biurko

W gabinecie kierownika stała nowa szafa pancerna, a obok niej wiadro zbierające wodę z przeciekającego sufitu.

— PANIE GRZESIU! POTRZEBUJEMY JESZCZE JEDNEGO FIREWALLA!

— Najpierw potrzebujemy dekarza.

— PRZECIEŻ DACH NIE JEST PODŁĄCZONY DO INTERNETU!

— Do dokumentów pod nim też nie trzeba Internetu, żeby je zalać.

Bezpieczeństwo zaczyna się od ustalenia, **co chronimy** (zasoby), **przed czym** (zagrożenia), **jakie słabości mogą zostać wykorzystane** (podatności) i **jakie mogą być skutki**. **Ryzyko** zależy między innymi od prawdopodobieństwa zdarzenia i jego konsekwencji. Niekiedy większym problemem od egzotycznego cyberataku jest brak kopii danych, awaria zasilania czy dostęp zbyt wielu osób do jednego konta.

— Czyli nie kupujemy trzydziestego firewalla?

— Nie teraz.

— A CO, JEŚLI KTOŚ ZAATAKUJE DACH?!

— Wtedy poprosimy dekarza o analizę podatności dachówek.

Hasło na kartce ma świetną dostępność

Pan Kierownik wydał nowe zarządzenie: hasła mają mieć trzydzieści znaków, być zmieniane codziennie i nie wolno ich nigdzie zapisywać.

W poniedziałek wszyscy zapisali je na karteczkach. We wtorek karteczki były już przyklejone pod klawiaturami. W środę recepcja prowadziła segregator „HASŁA — NIE OTWIERAĆ”.

— PANIE GRZESIU! DLACZEGO LUDZIE ŁAMIĄ PROCEDURY?!

— Bo pan stworzył procedurę, której nie da się wygodnie przestrzegać.

— TO ZAKAZUJĘ NIEWYGODY!

— Świetnie. Został pan pierwszym człowiekiem, który wydał rozporządzenie przeciwko rzeczywistości.

W praktyce warto stosować **długie, unikalne hasła**, menedżery haseł i **uwierzytelnianie wieloskładnikowe (MFA)**, a dodatkowo ograniczać próby logowania i reagować na podejrzenie przejęcia konta. Rutynowa, bardzo częsta zmiana silnych haseł bez powodu może sprzyjać przewidywalnym schematom i zapisywaniu ich w niebezpiecznych miejscach. Samo hasło nie powinno być jedyną linią obrony. Szczegóły zostawimy osobnemu artykułowi o hasłach i MFA.

Wszyscy są administratorami, bo kierownik ufa ludziom

Audytor poprosił o zestawienie uprawnień. Księgowa mogła zmieniać konfigurację serwera, magazynier kasować konta użytkowników, a Pan Kierownik miał uprawnienia do wszystkiego, choć nie pamiętał, do czego służy połowa przycisków.

— TO BUDUJE ZAUFANIE! — wyjaśnił.

— A komu jest potrzebne uprawnienie do usuwania kopii zapasowych? — zapytał Grzesiu.

— KAŻDEMU, KTO BĘDZIE CHCIAŁ POSPRZĄTAĆ!

— To tak, jakby dać wszystkim pracownikom klucze do sejfu, serwerowni i magazynu środków czystości.

— WŁAŚNIE! JEDEN KLUCZ, SAME OSZCZĘDNOŚCI!

Zasada **najmniejszych niezbędnych uprawnień** mówi, że użytkownik, program czy usługa powinny mieć tylko taki dostęp, jaki jest potrzebny do wykonywania swoich zadań. Warto rozdzielać obowiązki, używać osobnych kont administracyjnych, odbierać niepotrzebne uprawnienia i przeglądać je po zmianie stanowiska. Ograniczamy wtedy szkody wynikające zarówno z pomyłki, jak i z przejęcia konta.

Siedem kłódek i otwarte okno

Firma kupiła nową zaporę sieciową. Pan Kierownik zamówił także dodatkowy antywirus, drugą kamerę nad drzwiami i trzecią firmę ochroniarską.

— PO CO NAM TYLE WARSTW? — zapytała Agnieszka.

— BO KAŻDA ZATRZYMA HAKERA!

— A okno w magazynie? — spytał Grzesiu.

— JAKIE OKNO?

— To otwarte. Z kartką „PROSZĘ ZAMYKAĆ”.

— PROSZĘ NATYCHMIAST DODAĆ CZWARTĄ KAMERĘ!

— Może najpierw zamkniemy okno?

Obrona warstwowa oznacza stosowanie różnych, uzupełniających się środków: aktualizacji, kontroli dostępu, segmentacji sieci, monitorowania, ochrony urządzeń, edukacji, kopii zapasowych i przygotowania do incydentów. Żadna pojedyncza warstwa nie daje stuprocentowej gwarancji. Warstwy powinny odpowiadać rzeczywistym ryzykom, a nie stanowić konkursu na liczbę pudełek z napisem „SECURITY”.

Aktualizacja podczas przecinania wstęgi

W połowie odbioru system ochrony zaproponował aktualizację. Pan Kierownik, zachwycony nowym przyciskiem, kliknął „AKTUALIZUJ WSZYSTKO TERAZ”. Po chwili ekran zamigotał, drukarka wydrukowała pustą stronę, a kontrola wejść rozpoczęła restart.

— PANIE GRZESIU! CO SIĘ STAŁO?!

— Zrobił pan aktualizację całego systemu w środku uroczystości.

— PRZECIEŻ AKTUALIZACJE POPRAWIAJĄ BEZPIECZEŃSTWO!

— Tak. A zaplanowane okno serwisowe poprawia również szanse, że goście nie będą wychodzić przez okno.

Aktualizacje usuwają znane błędy i podatności, ale w ważnych środowiskach potrzebują planu: oceny pilności, testów tam, gdzie to możliwe, kopii lub planu wycofania zmian oraz wiedzy, co trzeba ponownie uruchomić. Odkładanie krytycznych poprawek bez końca jest ryzykowne; instalowanie wszystkiego bez przygotowania również.

Kopia zapasowa w tym samym płonącym sejfie

— A CO JEŚLI WSZYSTKO MIMO TO PADNIE?! — zapytał Kierownik.

— Odtworzymy dane z **kopii zapasowych** — odpowiedział Grzesiu.

— MAMY TRZY KOPIE!

— Gdzie?

— W TRZECH FOLDERACH NA TYM SAMYM DYSKU!

— A jeśli dysk się zepsuje?

— TO PROSZĘ ZROBIĆ CZWARTY FOLDER!

Agnieszka spojrzała na Grzesia. — Znowu będziemy rozmawiać o skarpetkach?

— Obawiam się, że tak.

Bezpieczeństwo obejmuje także **odporność i możliwość odtworzenia działania**. Przydają się niezależne kopie, odpowiednia retencja, kopie offline lub odseparowane uprawnieniami oraz regularne próby odzyskiwania. **RAID** pomaga przy wybranych awariach sprzętu, ale nie zastępuje backupu. Kopia, której nikt nie sprawdził, jest raczej obietnicą niż planem.

Alarm, którego nie wolno było zgłosić

Nagle na monitorze pojawił się komunikat o nietypowym logowaniu. Pan Kierownik kazał go wyciszyć, ponieważ przeszkadzał w przemówieniu.

— PANIE GRZESIU! NIECH PAN WYŁĄCZY TEN ALARM!

— Najpierw sprawdzimy, co oznacza.

— A JEŚLI TO FAŁSZYWY ALARM?

— To udokumentujemy i dostroimy regułę.

— A JEŚLI PRAWDZIWY?

— Ograniczymy dostęp, zabezpieczymy ślady, ocenimy zakres i przywrócimy usługę zgodnie z planem.

— NIE MOŻNA PO PROSTU NACISNĄĆ „WSZYSTKO BĘDZIE DOBRZE”?

— Ten przycisk mamy tylko na pańskim pulpicie.

Incydent wymaga **wykrycia, oceny, ograniczenia skutków, usunięcia przyczyny i odtworzenia działania**. Nie każdy alert oznacza włamanie, ale ignorowanie wszystkich to też nie strategia. Dobrze wiedzieć wcześniej, kto podejmuje decyzje, kogo zawiadomić, które systemy odizolować i jak zachować dowody. Po incydencie warto wyciągnąć wnioski, nie tylko znaleźć winnego.

Kto pilnuje pana kierownika?

Komisja poprosiła o plan szkoleń i zakres odpowiedzialności. Pan Kierownik wyciągnął dokument zatytułowany „ZASADY BEZPIECZEŃSTWA”. Miał jedno zdanie: „Pracownicy mają uważać”.

— A co robi pracownik, gdy dostanie podejrzaną wiadomość? — spytała komisja.

— UWAŻA!

— A gdy zgubi telefon służbowy?

— UWAŻA BARDZIEJ!

— A gdy ktoś podszyje się pod pana i poprosi o przelew? — zapytała Agnieszka.

— NIECH ZADZWONI DO MNIE!

— Właśnie o to chodzi — uśmiechnęła się księgowa. — Tylko warto to zapisać tak, żeby każdy wiedział.

Bezpieczeństwo to praca ludzi, procedur i technologii. Potrzebne są proste zasady, ćwiczenia, kultura zgłaszania błędów bez strachu przed automatyczną karą oraz jasna odpowiedzialność za decyzje. Użytkownik nie musi być specjalistą od kryptografii, żeby zauważyć podejrzaną prośbę. Zarząd nie musi administrować firewallem, ale powinien rozumieć ryzyko i zapewnić zasoby.

Finał: certyfikat stuprocentowego rozsądku

Po całym dniu komisja wróciła pod transparent. Pan Kierownik wyglądał na człowieka, który właśnie dowiedział się, że nie istnieje ubezpieczenie od własnych pomysłów.

— CZYLI NASZ BUDYNEK NIGDY NIE BĘDZIE W STU PROCENTACH BEZPIECZNY?

— Nie możemy uczciwie tego obiecać — odparł Grzesiu.

— TO PO CO NAM TE WSZYSTKIE ZABEZPIECZENIA?!

— Żeby zmniejszać ryzyko, ograniczać szkody i móc dalej działać, gdy coś zawiedzie.

— A CO WPISZEMY NA TRANSPARENCIE?!

Agnieszka podała mu flamaster.

— Może „MYŚLIMY, SPRAWDZAMY I ROBIMY KOPIE”?

— ZA MAŁO REKLAMOWE!

— Za to prawdziwe — zauważył audytor.

Pan Kierownik przez chwilę milczał, po czym triumfalnie uniósł rękę.

— JUŻ WIEM! NOWE HASŁO: „WSZYSTKO BĘDZIE DOBRZE, BO SPRAWDZILIŚMY, CO ZROBIĆ, KIEDY NIE BĘDZIE!”

Grzesiu spojrzał na Agnieszkę.

— Przyznaję. Pierwsza sensowna rzecz, którą dziś powiedział.

— ZAPISZCIE TO W PROTOKOLE! — rozkazał Kierownik.

— Już zapisaliśmy — odparła księgowa. — I zrobiliśmy kopię.

— GDZIE?!

— Nie w tym samym sejfie.

Bezpieczeństwo IT nie polega na obietnicy, że nic złego się nie wydarzy. Polega na świadomym chronieniu tego, co ważne, rozsądnym ograniczaniu ryzyka i gotowości do działania, kiedy zabezpieczenia zawiodą. A jeśli ktoś oferuje stuprocentową gwarancję, warto zapytać, czy przypadkiem nie sprzedaje również betonu do sejfu. 🤣

Protokół odbioru: budynek dopuszczono do dalszych prac po usunięciu usterek. Transparent „100% GWARANCJI” przekazano do działu marketingu. Grzesiu odzyskał kanapkę. Nie odzyskał urlopu. 🤣❤️