**Czytaj lub słuchaj artykuł online**

Zeskanuj kod QR, aby otworzyć artykuł na XO.PL

Źródło artykułu:

**https://xo.pl/it-na-wesolo-sec-policy**

BEZPIECZEŃSTWO IT

# Polityka bezpieczeństwa, czyli kto decyduje, kto wykonuje i kto odpowiada

W Urzędzie do Spraw Wszystkiego zbliżał się audyt bezpieczeństwa. Pan Kierownik zwołał zebranie i na środku stołu położył segregator wielkości małej lodówki. Na grzbiecie widniał złoty napis: „POLITYKA BEZPIECZEŃSTWA — WERSJA OSTATECZNA, TOM I Z XII". Agnieszka z księgowości odsunęła kubek. Grzesiu zaczął szukać wyjścia awaryjnego. 📋🔐🤣

— OD DZIŚ JESTEŚMY BEZPIECZNI! — oznajmił Kierownik.

— Co się zmieniło? — zapytała Agnieszka.

— WYDRUKOWALIŚMY POLITYKĘ!

— A hasła do księgowości?

— TE SAME!

— A kopie zapasowe?

— TEŻ TE SAME!

— A kto zgłasza incydent?

— JEST W SEGREGATORZE!

Grzesiu otworzył tom pierwszy. Przeczytał: „Każdy odpowiada za bezpieczeństwo w zakresie swoich kompetencji".

— Fantastycznie. Gdy coś się wydarzy, każdy będzie czekał, aż zrobi to ktoś inny.

## Segregator nie zatrzyma włamywacza

Kierownik ustawił dokumenty wzdłuż stołu jak fortyfikacje.

— POLITYKA, PROCEDURA, INSTRUKCJA, REGULAMIN UŻYWANIA REGULAMINÓW!

— Brakuje instrukcji otwierania segregatora — zauważyła Agnieszka.

— TOM SIÓDMY!

Grzesiu napisał na tablicy: „Co?", „Kto?", „Jak?".

**Polityka bezpieczeństwa informacji** wyznacza cele, zasady i odpowiedzialność. Procedury opisują konkretne działania, a instrukcje mogą wyjaśniać wykonanie poszczególnych czynności. Całość musi pasować do prawdziwej organizacji, nie do wyobrażeń autora.

— Czy samo podpisanie instrukcji przeciwpożarowej gasi pożar? — zapytał Grzesiu.

— NIE, ALE MAMY PODPIS!

— Podpis jest dowodem zatwierdzenia, nie dowodem skuteczności. Sprawdzimy ją po tym, co ludzie naprawdę robią.

## Wszyscy odpowiedzialni, czyli nikt konkretnie

W archiwum zepsuł się zamek. Kierownik wysłał wiadomość do wszystkich: „Pilnie naprawić!”. Każdy ją przeczytał. Nikt nie ruszył.

— WYDAŁEM POLECENIE!

— Wszystkim naraz — zauważyła Agnieszka. — A kto miał wykonać?

Grzesiu rozrysował podział ról.

— Musimy wiedzieć, kto podejmuje decyzję, kto wykonuje zadanie, kogo konsultujemy i kogo informujemy. Można użyć macierzy RACI albo prostszej tabeli. Najważniejsze, żeby odpowiedzialność była jednoznaczna.

— TO JA BĘDĘ ZATWIERDZAŁ WSZYSTKO!

— A gdy będzie pan na urlopie, firma nie zresetuje nikomu hasła? Kierownictwo określa cele i zapewnia zasoby. Właściciele systemów ustalają wymagania, administratorzy wdrażają ochronę, pracownicy stosują zasady i zgłaszają problemy.

— A ja? — zapytała Agnieszka.

— Pani wie, co się stanie, jeśli księgowość nie zadziała przed wypłatami. Bez wiedzy właściciela procesu nie ocenimy ryzyka.

— WSZYSTKO JEST KRYTYCZNE! — zawołał Kierownik.

— Wtedy nic nie jest priorytetem — odpowiedziała księgowa.

## Ściśle tajna zupa pomidorowa

Ministerialny segregator głosił, że wszystkie dokumenty są poufne. Łącznie z menu stołówki.

— Żeby poznać dzisiejszą zupę, pracownik musi złożyć wniosek? — spytała Agnieszka.

— BEZPIECZEŃSTWO WYMAGA WYRZECZEŃ!

— Ochrona powinna być proporcjonalna — wyjaśnił Grzesiu. — Publiczny cennik, dokument wewnętrzny, dane klienta i poufne informacje finansowe mają różne wymagania. Klasyfikacja informacji pomaga wybrać zasady dostępu, przechowywania i udostępniania.

— TO MOŻE ZUPA BĘDZIE PUBLICZNA?

— Chyba że stanowi plan tajnej operacji — odparła Agnieszka.

— KTO WPISAŁ ROSÓŁ DO AKT TAJNYCH?!

— Pan. Wczoraj o 14:07. Mam podpis.

## Ryzyko, którego nie da się zakazać

Kierownik zarządził ochronę przed wszystkim: złodziejami, powodzią, awarią prądu, pomyłką pracownika i meteorytem.

— NAJLEPIEJ ZAKAZAĆ METEORYTÓW!

— Meteor nie podpisywał regulaminu — zauważyła Agnieszka.

Grzesiu pokazał rejestr ryzyka.

— Oceniamy, co chronimy, co może się wydarzyć, jakie są skutki i prawdopodobieństwo oraz jaki poziom ryzyka organizacja jest gotowa zaakceptować. Potem dobieramy zabezpieczenia. Ryzyko można ograniczać, unikać go, czasem przenosić albo świadomie zaakceptować.

— KTO ZATWIERDZA AKCEPTACJĘ?

— Uprawniony właściciel ryzyka. Administrator może wskazać zagrożenie i możliwości techniczne, ale nie powinien sam decydować, ile strat firma jest gotowa ponieść.

— A JEŚLI NAPISZĘ „JAKOŚ TO BĘDZIE”?

— To nie jest nazwisko osoby odpowiedzialnej.

## Administrator dla każdego!

O dziesiątej Kierownik zapowiedział reformę dostępu.

— NIKOGO NIE BLOKUJEMY! WSZYSCY DOSTAJĄ ADMINISTRATORA!

— W takim razie najlepiej odebrać wszystkim komputery, żeby niczego nie zepsuli — zaproponowała Agnieszka.

— DOSKONAŁY POMYSŁ!

— Oba pomysły są złe — przerwał Grzesiu. — Zasada najmniejszych niezbędnych uprawnień oznacza dostęp tylko do tego, czego naprawdę wymaga praca. Księgowa nie musi zarządzać serwerami, a administrator nie musi czytać cudzej poczty.

Dostępy powinno się zatwierdzać, okresowo przeglądać i odbierać, gdy pracownik zmienia obowiązki albo odchodzi. Trzeba też zaplanować dostęp awaryjny, by nie tworzyć ukrytych furtek.

— JUŻ MAM FURTKĘ! KLUCZ JEST POD DONICZKĄ!

— Ten pomysł znamy z **hotelu „Pod Złotym Hasłem”** — westchnął Grzesiu. — I nie stał się lepszy.

## Wyjątek ważny do końca świata

W południe drukarka przestała działać. Kierownik chciał natychmiast wyłączyć wszystkie zabezpieczenia.

— WYŁĄCZYĆ FIREWALL! MUSZĘ WYDRUKOWAĆ RAPORT!

— Sprawdzimy, jakiego ruchu drukarka potrzebuje, co zostało zablokowane i jak zrobić możliwie wąski wyjątek — odpowiedział Grzesiu.

— A PO CO TYLE ZACHODU?

— Polityka zmian powinna mówić, kto zgłasza potrzebę, kto ocenia ryzyko, kto zatwierdza i wdraża, jak testujemy oraz jak cofamy zmianę, jeśli coś pójdzie źle. Wyjątki powinny mieć zakres, właściciela i często termin wygaśnięcia.

Agnieszka podniosła poprzedni formularz.

— Tu jest wpis: „Otworzyć wszystko, bo nie działa”. Bez daty i planu cofnięcia.

— KTO TO PODPISAŁ?!

— Pan. W Republice Pakietów.

— To dokładnie ta sama historia, co nasza **przygoda z firewallem** — uśmiechnął się Grzesiu.

## Incydent nie przychodzi z napisem „Incydent”

O 12:43 Agnieszka dostała wiadomość o pilnej zmianie rachunku dostawcy. Nie zrobiła przelewu. Zgłosiła wiadomość zgodnie z procedurą.

— A GDYBY TO NIE BYŁ OSZUST? — spytał Kierownik.

— Wtedy sprawdzimy. Pracownik nie musi sam przeprowadzać śledztwa. Musi wiedzieć, jak szybko zgłosić podejrzane zdarzenie — wyjaśnił Grzesiu.

Dobra procedura incydentowa wyznacza kanał kontaktu, osoby odpowiedzialne, sposób oceny pilności, zabezpieczenia informacji o zdarzeniu i komunikowania się z właściwymi ludźmi. Trzeba ją przetestować, zanim wydarzy się kryzys.

— TO ZROBIĘ PIECZĄTKĘ „NIE INCYDENT”! — oznajmił Kierownik.

— Pieczątka nie zastępuje oceny. A wiadomość wygląda jak przykład z naszego artykułu o **phishingu**.

## Backup z paragrafu dziewiątego

Audytor zapytał, kiedy ostatnio przywrócono dane z kopii zapasowej.

— W TOMIE DZIEWIĄTYM JEST NAPISANE, ŻE ROBIMY BACKUP!

— Kiedy testowaliśmy odtwarzanie? — zapytała Agnieszka.

Nastała cisza tak długa, że uruchomił się wygaszacz ekranu.

— Procedura robienia kopii to nie dowód, że da się odzyskać dane — powiedział Grzesiu. — Potrzebujemy harmonogramów, testów, odpowiedzialnych osób i ochrony kopii. Podobnie ze szkoleniami: potwierdzenie przeczytania regulaminu nie oznacza, że pracownik umie rozpoznać zagrożenie.

— ALE WYSŁALIŚMY REGULAMIN WSZYSTKIM!

— I czy wiedzą, co zrobić, gdy zgubią laptop albo otrzymają fałszywą wiadomość? Mamy osobne materiały o **backupie** i **podstawach bezpieczeństwa**. Polityka ma prowadzić do praktyki, nie tylko do wysyłki PDF-a.

## Audytor chce dowodów, nie kilogramów papieru

Na audycie Kierownik z dumą ustawił dwanaście segregatorów od największego do najmniejszego.

— NASZE BEZPIECZEŃSTWO WAŻY SIEDEMNAŚCIE KILOGRAMÓW!

— Czy mogę zobaczyć ostatni przegląd uprawnień? — zapytał audytor.

— TOM TRZECI!

— Wyniki testu odtwarzania?

— TOM DZIEWIĄTY!

— A czy ktoś te działania wykonał?

Zapadła cisza. Agnieszka przyniosła rejestr zmian, listę odpowiedzialnych osób i raport z testu odtwarzania przeprowadzonego po porannej rozmowie.

— Właśnie o to chodzi — powiedział audytor. — Dokument opisuje zamiar, a dowody i praktyka pokazują wykonanie. Sam pozytywny audyt nie gwarantuje, że nigdy nic się nie wydarzy.

— TO CO Z SEGREGATORAMI?!

— Mogą zostać. Ale proszę, żeby ludzie potrafili znaleźć potrzebną informację szybciej niż w trzy dni.

## Polityka do używania, nie do podziwiania

Wieczorem Agnieszka przygotowała krótsze zasady z jasnymi odnośnikami do procedur. Wskazała właścicieli, sposób zgłaszania problemów, ścieżkę wyjątków i terminy przeglądów.

— Czyli nie trzeba znać dwunastu tomów na pamięć? — zapytał recepcjonista.

— Wystarczy wiedzieć, jak bezpiecznie pracować, czego nie robić i gdzie szukać pomocy — odpowiedział Grzesiu. — Dokumenty muszą być dostępne, zrozumiałe, aktualne i dopasowane do firmy.

— A jeśli wszystko się zmieni? — zapytała Agnieszka.

— Przeglądamy politykę po istotnych zmianach i w zaplanowanych terminach. Nie powinna opisywać serwera, którego od pięciu lat nie ma.

— MOŻE JEDNA ZASADA: „PROSZĘ MYŚLEĆ”?! — zaproponował Kierownik.

— Dobra rada, ale nie zastąpi określenia uprawnień, odpowiedzialności i procedur.

— TO JA JESZCZE PRZYBIJĘ PIECZĄTKĘ!

Uderzył w biurko tak mocno, że z segregatora wypadła karteczka: „Hasło administratora — proszę pytać Kierownika”.

— WIDZICIE?! CENTRALIZACJA ODPOWIEDZIALNOŚCI!

— Nie — odpowiedziała Agnieszka. — To zadanie na kolejny przegląd.

**Polityka bezpieczeństwa nie jest tarczą z papieru. Ma określać rozsądne zasady, właścicieli decyzji i sposób działania. Zbyt rozbudowana staje się martwa, zbyt ogólna niczego nie wyjaśnia, a niewykonywana daje tylko złudzenie ochrony.**

---

*Protokół Urzędu do Spraw Wszystkiego: polityka ma właściciela, wyjątki mają terminy ważności, incydenty mają adres zgłoszeniowy, a kopie zapasowe harmonogram testów. Dwanaście segregatorów zostało w archiwum. Pan Kierownik złożył wniosek o trzynasty: „Polityka ochrony przed nadmiarem polityk”. Wniosek czeka na jego własny podpis.* 📋🤣❤️