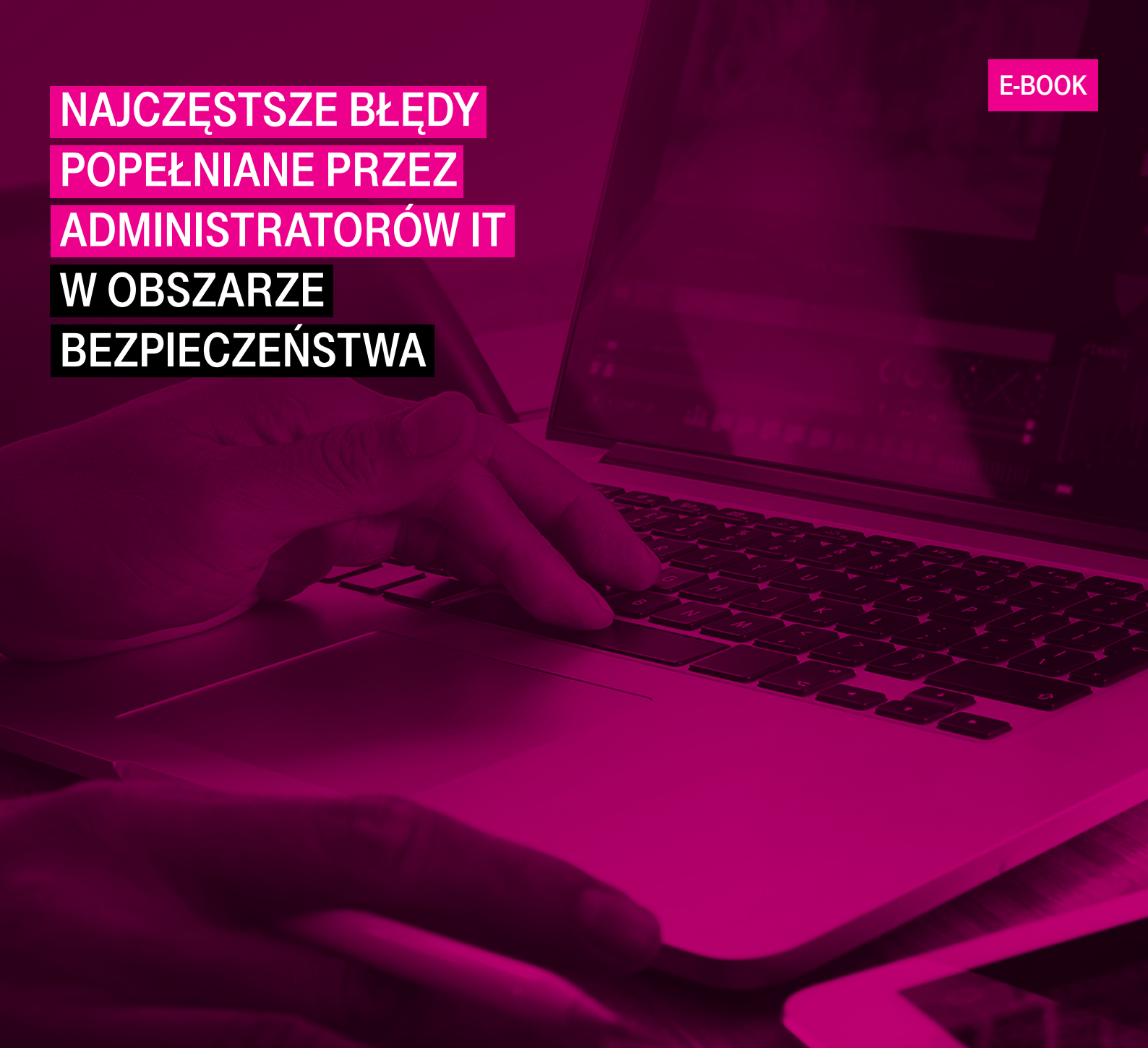
E-BOOK

NAJCZĘSTSZE BŁĘDY POPEŁNIANE PRZEZ ADMINISTRATORÓW IT W OBSZARZE BEZPIECZEŃSTWA



SPIS TREŚCI

W powszechnym przekonaniu przyczyną udanych cyberataków i wycieków danych są głównie błędy popełniane przez użytkowników systemów. Nie jest to teoria pozbawiona uzasadnienia, jednak istnieje także inne, rzadziej opisywane źródło problemów. Choć prawdopodobnie więcej błędów w systemach i aplikacjach IT popełniają ich użytkownicy, to należy pamiętać, że błędy popełnione przez administratorów mogą mieć dużo poważniejsze konsekwencje dla bezpieczeństwa IT organizacji.

1. Co jest najczęstszą przyczyną cyberataków
2. Jakie mechanizmy uwierzytelniające cyberprzestępcy atakują najczęściej
3. Jakie błędy najczęściej popełniają administratorzy
4. Jakie konsekwencje dla bezpieczeństwa it organizacji mają błędy popełniane przez administratorów

Jest kilka powodów, dla których pomyłki lub zaniedbania administratorów powinny być szczególnie brane pod uwagę podczas analizy ryzyka IT. Po pierwsze, osoby zarządzające rozwiązaniami IT mają z racji pełnionych obowiązków dużo większe uprawnienia, pozwalające często nie tylko na pełną kontrolę nad systemami, ale także na ukrycie śladów ewentualnych incydentów. Po drugie, administratorzy często przekonani są o tym, że błędy bezpieczeństwa popełniają użytkownicy a informatyków te problemy zwyczajnie nie dotyczą. Po trzecie, cyberprzestępcy chętnie wykorzystują błędy popełniane przez specjalistów IT – to szybki i efektywny kosztowo sposób pokonania mechanizmów uwierzytelniających atakowanej firmy. Te powody sprawiają, że warto przyjrzeć się błędom najczęściej popełnianym przez administratorów.

NASZE HASŁA SĄ BEZPIECZNE

Hasła są jednym z podstawowych mechanizmów zapewniających bezpieczeństwo danych. Prawidłowe ich tworzenie, przechowywanie, zarządzanie i używanie stanowią jednak spore wyzwanie - także dla administratorów.

Polscy informatycy do tej pory pamiętają wykradzione przez włamywaczy hasło broniące dostępu do oficjalnej strony internetowej Kancelarii Premiera RP, „admin1". Podobne trywialne hasła często padają ofiarami automatów skanujących Internet i odgadujących hasła do popularnych usług takich jak SSH (ang. secure shell czyli standard protokołów komunikacyjnych używanych w sieciach komputerowych TCP/IP) czy RDP (ang. Remote Desktop Protocol - protokół pozwalający na komunikację z usługą terminala graficznego w Microsoft Windows). Czasem administratorzy pozwalają sobie na ustawienie „na chwilkę" prostego hasła do usługi dostępnej z zewnątrz, zakładając, że nic złego w tym czasie się nie stanie. Niestety automaty skanujące sieć są bardzo szybkie i natarczywe, co powoduje, że proste hasło może zostać sprawdzone w ciągu kilku sekund po jego ustawieniu. Nawet jeśli administrator po chwili ponownie ustawi bezpieczne hasło, to na serwerze może być już zainstalowane złośliwe oprogramowanie.

NIE MAMY WŁAMYWACZY W SIECI WEWNĘTRZNEJ

Innym popularnym, lecz niebezpiecznym podejściem jest ustawianie prostych haseł w sieci wewnętrznej firmy. Cześć administratorów wychodzi z błędnego założenia, że użytkownicy w firmowej sieci nie są zagrożeniem. O ile faktycznie rzadko zdarza się, by to pracownik włamywał się do wewnętrznych systemów (częściej wykorzystują oni już posiadane dostępy), to jeśli do firmowej sieci raz dostanie się włamywacz, proste hasła znacznie ułatwiają mu uzyskanie dostępu do innych systemów i mogą znacząco zwiększyć straty. W ograniczeniu tego zagrożenia może pomóc separacja sieci wewnętrznych, lecz nie oznacza to, że można w niej stosować łatwiejsze hasła.

PO CO MI RÓŻNE HASŁA?

Kolejnym grzechem administratorów jest używanie tych samych haseł w wielu różnych miejscach. Do ogromnego wycieku danych użytkowników Dropboxa doszło dlatego, że jeden z administratorów używał tego samego hasła w różnych serwisach internetowych oraz do swojego firmowego konta na GitHubie. W podobny sposób wykradziono dane klientów Ubera. Przestępcy przeglądają zbiory wykradzionych danych użytkowników różnych serwisów poszukując w nich profili administratorów różnych firm, licząc na to, że z użyciem ich prywatnych haseł będą mogli dostać się także doe-book zasobów firmowych. W ten właśnie sposób przejęto nawet konto Marka Zuckerberga na Twitterze – używał tam tego samego hasła, jakim posługiwał się w serwisie LinkedIn.

TO TAM BYŁO DOMYŚLNE HASŁO?

Chyba najgorszym, ale niestety nadal często spotykanym zaniedbaniem jest pozostawienie domyślnych haseł dostępu ustawionych przez producenta sprzętu lub oprogramowania. W sieci łatwo można znaleźć spisy takich domyślnych ustawień, posortowane według producentów, modeli urządzeń czy rodzajów aplikacji. Pominięcie zmiany domyślnego hasła w procesie instalacji i konfiguracji urządzenia lub aplikacji jest tożsame z wystawieniem go na skuteczne ataki nawet początkujących włamywaczy. Szczególnie urządzenia dostępne z sieci publicznej z domyślnymi hasłami często stają się częścią botnetów (grupą komputerów zainfekowanych szkodliwym oprogramowaniem).

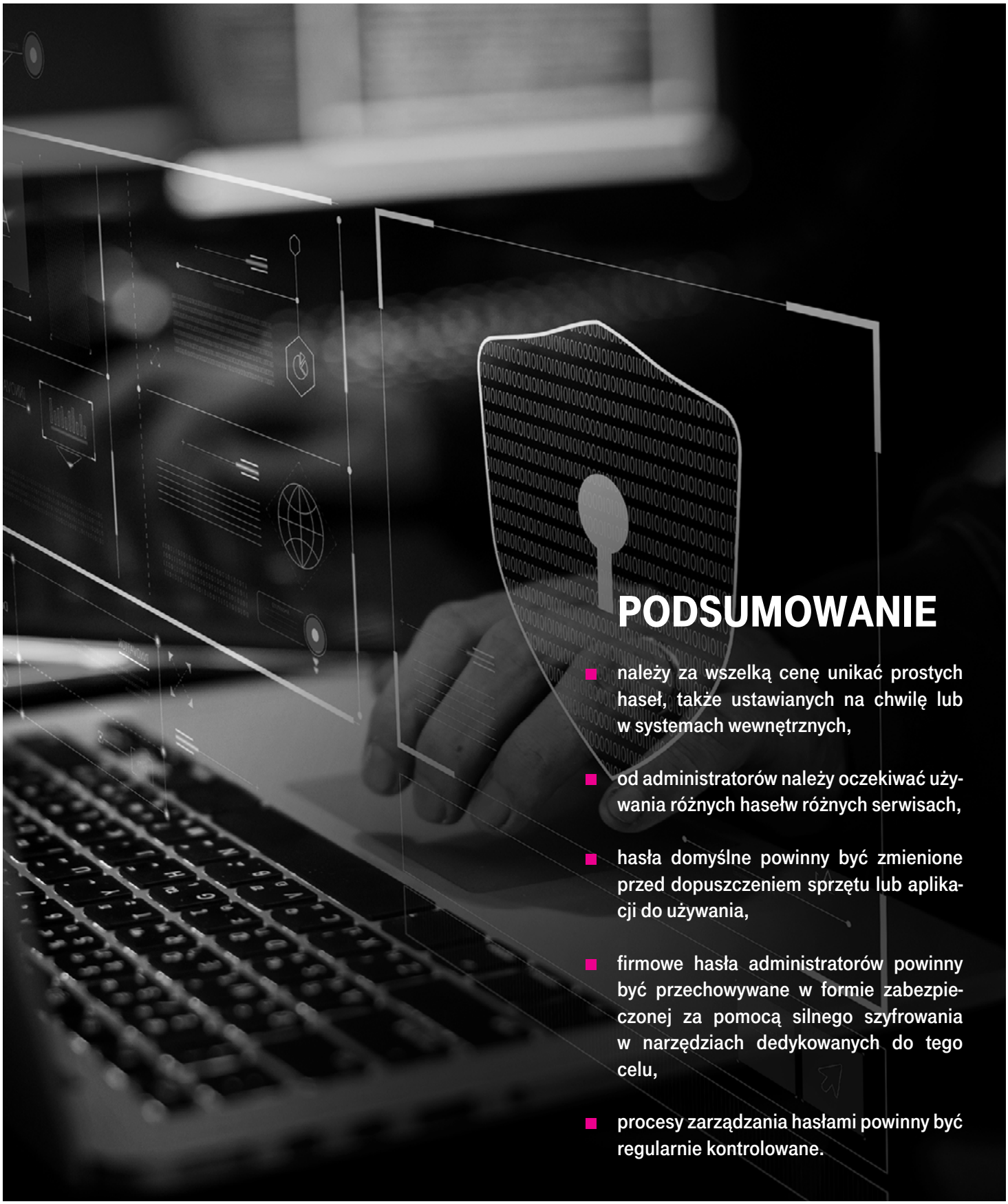
TRZYMAMY WSZYSTKO W EXCELU LUB NOTATNIKU

Piątym spośród najpoważniejszych grzechów administratorów dotyczących haseł jest nieprawidłowe przechowywanie danych uwierzytelniających. Czasem jednym z pierwszych (a także ostatnich) kroków testów penetracyjnych jest odnalezienie pliku tekstowego lub arkusza kalkulacyjnego zawierającego wszystkie hasła całego zespołu administratorów w jednym miejscu. Istnieje wiele narzędzi takich jak Dashlane czy Keeper, wspomagających prawidłowe szyfrowanie, zarządzanie hasłami. Ich stosowanie w środowiskach firmowych powinno być normą, a nie wyjątkiem.

LEPIEJ ZAPOBIEGAĆ ZAWCZASU

Odkrycie wszystkich złych praktyk dotyczących haseł stosowanych w danej firmie nie jest prostym zadaniem. Można podejść do tego z kilku różnych perspektyw. Po pierwsze, należy stworzyć odpowiednie standardy i procedury opisujące tworzenie, przechowywanie i zarządzanie hasłami. Po drugie, warto okresowo przeprowadzać audyty oraz testy penetracyjne, które pomagają w wykryciu nieprawidłowości w stosowaniu procedur. Trzecim elementem może być monitoring użycia haseł na poziomie systemu SIEM, pozwalający na wykrycie anomalii mogących stanowić zagrożenie bezpieczeństwa. Czwartym czynnikiem minimalizującym ryzyko i wartym rozważenia jest wdrożenie Web Application Firewall, który pozwoli ograniczyć ryzyko przełamywania zabezpieczeń aplikacji WWW, w tym prób odgadywania haseł.

Bezpieczeństwo haseł pozwala także znacząco podnieść wdrożenie wieloskładnikowego uwierzytelnienia. Nie zapominajmy także o zasadzie ograniczonego zaufania, która obowiązuje także w przypadku administratorów. W ich przypadku warto rozważyć użycie systemów zarządzania uprzywilejowanymi kontami oraz użytkownikami, pozwalających na ewidencjonowanie oraz monitorowanie zasadności przeprowadzanych przez nich operacji.



PODSUMOWANIE

- należy za wszelką cenę unikać prostych haseł, także ustawianych na chwilę lub w systemach wewnętrznych,
- od administratorów należy oczekiwać używania różnych hasełw różnych serwisach,
- hasła domyślne powinny być zmienione przed dopuszczeniem sprzętu lub aplikacji do używania,
- firmowe hasła administratorów powinny być przechowywane w formie zabezpieczonej za pomocą silnego szyfrowania w narzędziach dedykowanych do tego celu,
- procesy zarządzania hasłami powinny być regularnie kontrolowane.

KONFIGURACJA

Administratorzy systemów i aplikacji, podobnie jak inni użytkownicy, także popełniają błędy. Czasem wynikają one z niewiedzy, czasem zaniedbania, mogą też być skutkiem zbyt dużej liczby zadań do wykonania. Prawidłowe skonfigurowanie systemów, usług i aplikacji jest bardzo złożonym zadaniem i trudno jest zrobić to perfekcyjnie. O ile błędy użytkowników z reguły nie mają katastrofalnych skutków, to błędy administratorów mogą z większym prawdopodobieństwem prowadzić do poważnych incydentów bezpieczeństwa.

1. Jak ważne dla każdej organizacji jest prawidłowa konfiguracja serwera czy aplikacji
2. Jakie są podstawowe zasady bezpieczeństwa zasobów firmy
3. Jakie skutki niesie ze sobą domyślna konfiguracja serwera czy aplikacji
4. Czym grozi niewycofanie z użytkowania starych wersji oprogramowania czy niepotrzebnych plików na serwerach
5. Jakie są najważniejsze zalecenia dotyczące dbania o prawidłową konfigurację systemów i aplikacji

Celem prawidłowej konfiguracji serwera czy aplikacji jest ograniczenie możliwości ataków i utrudnienie zadania napastnikom. Aby zapewnić właściwy poziom ochrony zasobów organizacji niezbędne jest przestrzeganie podstawowych zasad bezpieczeństwa takich jak udostępnianie informacji tylko tym użytkownikom, którzy ich potrzebują czy usuwanie niepotrzebnych komponentów środowiska IT. Doświadczenie pokazuje jednak, że nie jest to proste.

DOMYŚLNE KONFIGURACJE

Mimo dużego postępu w tym obszarze nadal wielu dostawców usług czy oprogramowania nie zapewnia domyślnie ich bezpiecznej konfiguracji. Prawidłowe ustawienie zasad dostępu pozostaje zadaniem klienta, który nie zawsze potrafi mu podołać, co powoduje tysiące incydentów wycieków informacji rocznie.

Jednym z najczęściej spotykanych scenariuszy jest udostępnienie całemu światu repozytoriów danych w usługach chmurowych takich jak np. AWS. Taki błąd był powodem ujawnienia danych polskiej firmy pośredniczącej w rozliczaniu zdarzeń ubezpieczeniowych, ale także amerykańskich firm zbrojeniowych czy urzędów. Z kolei udostępnianie w sieci baz MongoDB w domyślnej konfiguracji bez hasła zaowocowało masowymi atakami ransomware, gdzie napastnicy szyfrowali lub usuwali dane i żądali okupu za ich odzyskanie.

Także domyślna konfiguracja bramek VoIP stała za stratami idącymi w miliony euro, gdy przestępcy wykorzystali cudze urządzenia do generowania wysokopłatnych połączeń. Skanowanie sieci pod kątem podobnych błędów jest ulubionym zajęciem wielu włamywaczy.

ZAPOMNIANE SERWERY, USŁUGI I SYSTEMY

O ile w przypadku uruchamiania lub aktualizacji nowych usług czy systemów z reguły ktoś pilnuje, czy już wystartowały, o tyle ich wycofanie z użytkowania często przebiega bez nadzoru i nikomu nie zależy na ich ostatecznym wyłączeniu. Mogą temu zaradzić zarówno dobre procedury jak i dedykowane narzędzia wspierające proces inwentaryzacji zasobów IT.

Podobny problem dotyczy starych wersji oprogramowania i niepotrzebnych plików na serwerach. W trakcie testów penetracyjnych nie raz można znaleźć na serwerze WWW kopie bazy danych sprzed kilku lub kilkunastu miesięcy, którą administrator wystawił do pobrania, a po pobraniu zapomniał usunąć.

Innym często spotykanym problemem jest publiczne udostępnianie testowych lub deweloperskich wersji aplikacji. Taki incydent dotknął m.in. system wyborczy w Polsce kilka lat temu. Z kolei włączona rozszerzona diagnostyka błędów, pomocna w ustalaniu przyczyn problemów technicznych, może pomóc włamywaczom w uzyskaniu dostępu do informacji dla nich nieprzeznaczonych. Taki incydent miał miejsce w popularnym polskim serwisie Kinoman, gdzie komunikat o błędzie bazy danych ujawniał login i hasło jej administratora. Warto tu zaznaczyć, że problem zarządzania hasłami pomagają rozwiązać dedykowane narzędzia, wymuszające przestrzeganie polityk bezpieczeństwa w tym obszarze.

ZARZĄDZANIE DOSTĘPEM

Przestępcy chętnie wykorzystują także nieprawidłowo skonfigurowane prawa dostępu. Brak ograniczeń przeciwko próbom odgadywania hasła znacząco ułatwia ataki typu bruteforce, gdzie włamywacze testują różne kombinacje loginów i haseł, aż znajdą prawidłowe. Listy najpopularniejszych haseł są publicznie dostępne w internecie i przestępcy często z nich korzystają.

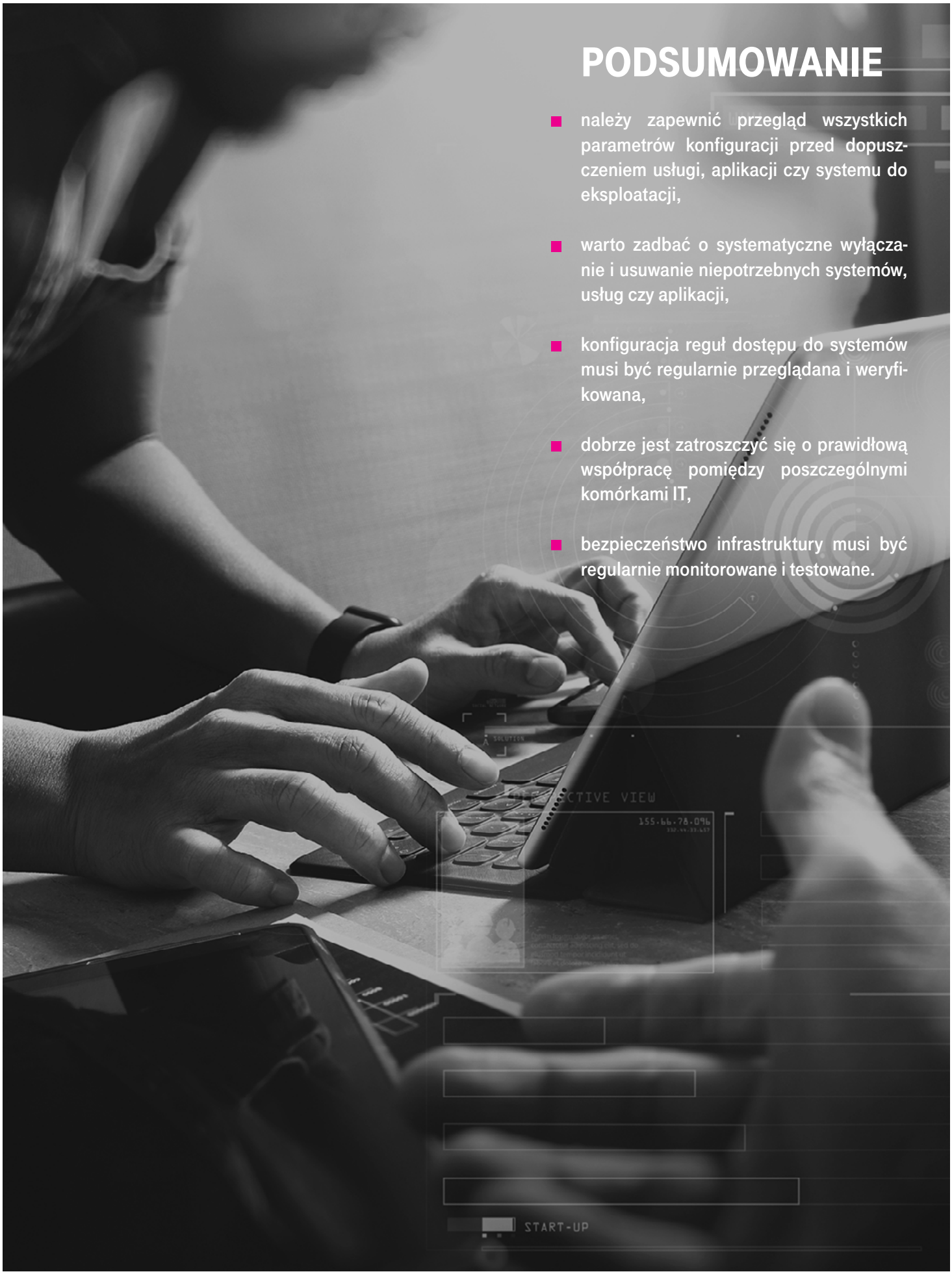
Z kolei w trakcie prób ustalania przyczyn problemów z łącznością sieciową dość popularnym krokiem jest łagodzenie reguł firewalla, aż do całkowitego przepuszczenia ruchu bez żadnej kontroli. Niestety zdarza się, że taka konfiguracja pozostaje na urządzeniu dłużej, niż jest to potrzebne, ułatwiając zadanie przestępcom. Taki incydent przydarzył się nawet jednemu z producentów firewalli, a problemy z właściwą konfiguracją reguł zabezpieczenia sieci leżały u podstaw niedawnej poważnej awarii systemów na lotnisku Okęcie.

PROGRAMIŚCI KONTRA ADMINISTRATORZY

Problemów z konfiguracją serwerów czy aplikacji nie łagodzą częste konflikty na linii programiści – administratorzy. Szybkie tempo rozwoju aplikacji, często przy użyciu gotowych modułów dostępnych w sieci, trudno pogodzić z zapisami procedur zarządzania systemami. Jeśli obie strony nie potrafią dojść do porozumienia, często kończy się to powstaniem „alternatywnego IT", bez oficjalnego wsparcia działów do tego dedykowanych, co nie wpływa pozytywnie na poziom bezpieczeństwa całej organizacji.

LEPIEJ ZAPOBIEGAĆ ZAWCZASU

Jak przeciwdziałać podobnym problemom? Bez wątpienia właściwie skonstruowane i wdrożone procedury są podstawowym elementem bezpieczeństwa. Z uwagi jednak na stopień skomplikowania problemu warto także zapewnić mechanizmy monitorowania sieci i nietypowych sytuacji takie jak Security Operations Center oraz mechanizmy prewencji, takie jak odpowiednio skonfigurowane i zarządzanie firewalle sieciowe oraz aplikacyjne. W ocenie stanu rzeczy pomogą także testy penetracyjne.



PODSUMOWANIE

- należy zapewnić przegląd wszystkich parametrów konfiguracji przed dopuszczeniem usługi, aplikacji czy systemu do eksploatacji,
- warto zadbać o systematyczne wyłączanie i usuwanie niepotrzebnych systemów, usług czy aplikacji,
- konfiguracja reguł dostępu do systemów musi być regularnie przeglądana i weryfikowana,
- dobrze jest zatroszczyć się o prawidłową współpracę pomiędzy poszczególnymi komórkami IT,
- bezpieczeństwo infrastruktury musi być regularnie monitorowane i testowane.

KOPIE BEZPIECZEŃSTWA

Kopie zapasowe są najpopularniejszym mechanizmem bezpieczeństwa spotykanym praktycznie we wszystkich polskich firmach. Znane są od kilkudziesięciu lat, o ich wykonywaniu napisano tysiące artykułów i poradników, wydawałoby się, że każdy administrator potrafi sobie z nimi świetnie poradzić i trudno popełnić w ich przypadku poważne błędy– a mimo tego leżą u podstaw dziesiątek wpadek i katastrof. Dlaczego?

1. Dlaczego warto dokładnie zaplanować zakres i częstotliwość tworzenia kopii zapasowych
2. Jakie skutki może mieć zaniechanie regularnego testowania prawidłowości odtwarzania kopii zapasowych
3. Czy regularne przeprowadzanie testów penetracyjnych pomaga wykryć potencjalne słabe punkty bezpieczeństwa infrastruktury i organizacji
4. Jakich zaleceń w zakresie tworzenia kopii bezpieczeństwa należy przestrzegać

PRZECIEŻ NA PEWNO MAMY BACKUPY

Wiara w to, że kopie bezpieczeństwa są wykonywane regularnie, prawidłowo i w sposób umożliwiający ich odzyskanie w wielu przypadkach okazuje się nie być oparta na faktach, a jedynie na przeświadczeniu, że wszystko jest w porządku.

Backupy, podobnie jak każdy mechanizm bezpieczeństwa, należy regularnie testować. Jest mnóstwo powodów, dla których kopie bezpieczeństwa mogą nie zostać prawidłowo wykonane. Uszkodzenia nośników, nieprawidłowe definicje zadań backupowych, błędy w skryptach, przepełnienie dysków, awarie sieciowe czy wreszcie zwykłe pomyłki operatora nie raz już były przyczyną niejednej niemiłej niespodzianki. Dlatego ignorowanie komunikatów o błędach w procesie wykonywania backupów nie pomaga w diagnostyce problemu. Co więcej, czasem błędy mogą być tak specyficzne, że raporty wskazują na prawidłowe tworzenie kopii zapasowej, podczas gdy w rzeczywistości dane nie zostały nawet skopiowane.

Taka sytuacja spotkała między innymi autorów animacji Toy Story 2, którzy po awarii dysków, w obliczu utraty całego materiału prawie gotowego już filmu, przez wiele miesięcy odtwarzali klatkę po klatce z fragmentarycznych kopii bezpieczeństwa, utworzonych przez przypadek dodatkowo przez jednego z pracowników.[1] Przed takimi ryzykami ustrzec firmę może tylko regularne testowanie pełnego procesu przywracania kopii zapasowych.

KOPIA JEST, ALE NIEAKTUALNA

Częstotliwość tworzenia kopii bezpieczeństwa może mieć kluczowe znaczenie dla jej przydatności w sytuacji awaryjnej. O ile archiwum zamówień klientów sprzed roku nie musi być backupowane codziennie, o tyle utrata bieżących zamówień nawet z ostatnich kilku godzin może powodować istotne straty dla firmy.

Czas poświęcony na analizę faktycznych potrzeb w zakresie sporządzania kopii zapasowych poszczególnych systemów może w przyszłości zwrócić się z nawiązką. Warto określić, co chcemy backupować, jak często, gdzie przechowywać zapasowe kopie a także jak szybko będziemy musieli dane odzyskać w przyszłości i dostosować używane technologie do tych wymagań.

KOPIA BYŁA, ALE JUŻ JEJ NIE MA

Może się też zdarzyć tak, że firma, mimo posiadania prawidłowo wykonanej kopii bezpieczeństwa, traci wszystkie dane. Najczęściej jest to efekt działania osoby o złych intencjach – włamywacza lub niezadowolonego pracownika. Znane są liczne przypadki ataków ransomware, które szyfrowało nie tylko podstawowe systemy firmy, ale także jej kopie zapasowe, by zwiększyć szansę otrzymania okupu przez szantażystów.

Przechowywanie kopii bezpieczeństwa na urządzeniach czy nośnikach dostępnych w trybie online jest bez wątpienia wygodne, jednak skutki takiego działania mogą okazać się opłakane, gdy dostanie się do nich włamywacz. Także rozproszenie geograficzne kopii online może okazać się niewystarczające – w ataku NotPetya firma Maersk utraciła wszystkie kopie serwera Active Directory, mimo, iż działał on równolegle w ponad 100 lokalizacjach. Tylko dzięki niezwykłemu szczęściu poszkodowana firma zawdzięcza fakt, że w momencie ataku serwery w Ghanie pozbawione były zasilania, dzięki czemu nie zostały zaszyfrowane razem z pozostałymi.[2]

Nie wszyscy jednak mają tyle szczęścia – amerykańska firma Code Spaces musiała zakończyć swoją działalność po tym, jak tajemniczy włamywacz usunął wszystkie jej dane oraz kopie zapasowe.[3]

1 https://thenextweb.com/media/2012/05/21/how-pixars-toy-story-2-was-deleted-twice-once-by-technology-and-again-for-its-own-good/
2 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
3 https://www.networkcomputing.com/cloud-infrastructure/code-spaces-lesson-cloud-backup/314805651

BACKUP JAKO NARZĘDZIE WŁAMYWACZA

W wielu atakach to właśnie nieprawidłowo zabezpieczone kopie bezpieczeństwa były wektorem włamania lub znaczną pomocą dla atakujących. Backupy umieszczone na publicznie dostępnym serwerze, zawierające hasła administratorów czy stare kopie plików konfiguracyjnych ujawniających hasła dostępowe do bazy danych są popularnym pierwszym krokiem w wielu atakach.

Nie raz także to właśnie błędy w oprogramowaniu czy urządzeniach do tworzenia kopii bezpieczeństwa pozwalały włamywaczom na przejęcie pełnej kontroli nad atakowaną infrastrukturą IT. Warto zatem pamiętać o tym, by regularnie stosować odpowiednie aktualizacje oprogramowania oraz przeprowadzać testy penetracyjne, pomagające wykryć potencjalne problemy bezpieczeństwa.

PODSUMOWANIE

Przed utratą danych na skutek awarii nie uchronili się nawet tacy giganci jak Google czy Amazon. Co zatem możemy zrobić, by do nich nie dołączyć? Można między innymi zlecić wykonywanie usługi kopii zapasowej specjalistom, np. w usłudze Backup oferowanej przez T-Mobile).

- **należy prawidłowo zaplanować zakres i częstotliwość tworzonych backupów,**
- **należy regularnie testować prawidłowość odtwarzania kopii bezpieczeństwa najważniejszych danych i systemów,**
- **dostęp do backupów powinien być maksymalnie ograniczony a przynajmniej jedna kopia powinna być przechowywana offline, w innej lokalizacji,**
- **narzędzia backupowe powinny być regularnie aktualizowane,**
- **niepotrzebne kopie należy bezzwłocznie usuwać.**

ZARZĄDZANIE UPRAWNIENIAMI

Zarządzanie dostępem do systemów oraz aplikacji jest trudnym zadaniem bez względu na rozmiar organizacji.

W dużych firmach problemy generuje często skala zjawiska – przy setkach systemów, tysiącach pracowników i ich znacznej rotacji zarządzanie ich uprawnieniami wiąże się z dłuższym od oczekiwanego czasem nadawania czy odbierania uprawnień oraz z ryzykiem popełnienia błędów. W średnich firmach wyzwaniem jest najczęściej ustalenie odpowiedzialności za ten proces – administratorzy obarczeni są wieloma zadaniami i zarządzanie uprawnieniami rzadko znajduje się wysoko na liście ich priorytetów. Z kolei w małych firmach głównym problemem jest brak możliwości rozdzielenia uprawnień pomiędzy różnych pracowników, co powoduje wyższe ryzyko nadużyć.

1. Jak istotne jest zarządzanie dostępami do systemów i aplikacji
2. Dlaczego właściciele systemów wolą przyznawać dużą liczbę uprawnień wykraczającą za zakres odpowiedzialności pracowników i jaki ma to wpływ na organizację i jej bezpieczeństwo
3. Dlaczego okresowe raporty z uprawnieniami przyznanymi pracownikowm mogą pomóc w terminowym odbieraniu im uprawnień
4. Czym jest macierz konfliktujących uprawnień
5. Czy automatyzacja zarządzania dostępami do systemów i aplikacji może rozwiązać problemy generowane przez proces zarządzania uprawnieniami.

TRUDNE SŁOWO MINIMALIZACJA

Podstawową zasadą zarządzania uprawnieniami jest nadawanie ich wyłącznie w niezbędnym zakresie. Nie da się ukryć, że dużo łatwiej jest to powiedzieć, niż faktycznie zrobić. Z jednej strony pracownicy, poza stanowiskami niskiego szczebla, często mają dość szerokie zakresy odpowiedzialności, a z drugiej strony konieczność regularnego dodawania i odbierania uprawnień w związku z ciągle zmieniającymi się potrzebami użytkowników motywuje właścicieli systemów by uprawnień przyznać więcej i oszczędzić sobie w przyszłości biurokracji. Niestety przyznawanie zbyt wielu uprawnień może się łatwo zemścić na organizacji. Co więcej, przy braku odpowiedniego nadzoru zdarzają się przypadki nadawania uprawnień bez przestrzegania firmowych procedur. Administrator systemu, który może jednocześnie manipulować logami, będzie w stanie dokonać nadużycia a następnie usunąć jego ślady. Pracownik, który może jednocześnie zgłaszać wydatki i je zatwierdzać, z łatwością będzie mógł

wyłudzać nienależne zwroty z firmowej kasy. Zmuszenie pracowników by w razie próby dokonania nadużycia musieli działać w większej grupie znacząco zmniejsza prawdopodobieństwo zajścia takiego incydentu oraz zwiększa szanse jego wykrycia.

ŁATWO NADAĆ, TRUDNIEJ ODEBRAĆ

Jednym z najczęściej spotykanych problemów w obszarze zarządzania uprawnieniami jest nie ich nadawanie, a odbieranie. Można to wyjaśnić w bardzo prosty sposób – o ile pracownik, któremu uprawnień brakuje będzie najczęściej ubiegał się o ich przyznanie tak długo, aż je otrzyma, o tyle pracownik, który ma za dużo uprawnień, z reguły nie ma żadnego interesu w dbaniu o pozbycie się ich nadmiaru.

Nadmiarowe uprawnienia w pracy nie przeszkadzają, a wręcz mogą się czasem przydać. Interes w dbaniu o terminowe odbieranie niepotrzebnych uprawnień powinien mieć gestor systemu – czyli osoba, która odpowiada za zawarte w nim dane i zarządzanie dostępem do nich. Niestety bardzo często jest to osoba zajęta innymi obowiązkami i nie dysponuje czasem, by problemowi odbierania uprawnień bliżej się przyjrzeć.

Podobnym problemem jest odbieranie uprawnień osobom, które odchodzą z pracy. Czasem zdarza się, że były pracownik nadal ma dostęp zdalny do różnych systemów lub może np. przekierować pocztę ze swojego starego konta na nowe i odbierać emaile jeszcze wiele miesięcy po ustaniu stosunku pracy.

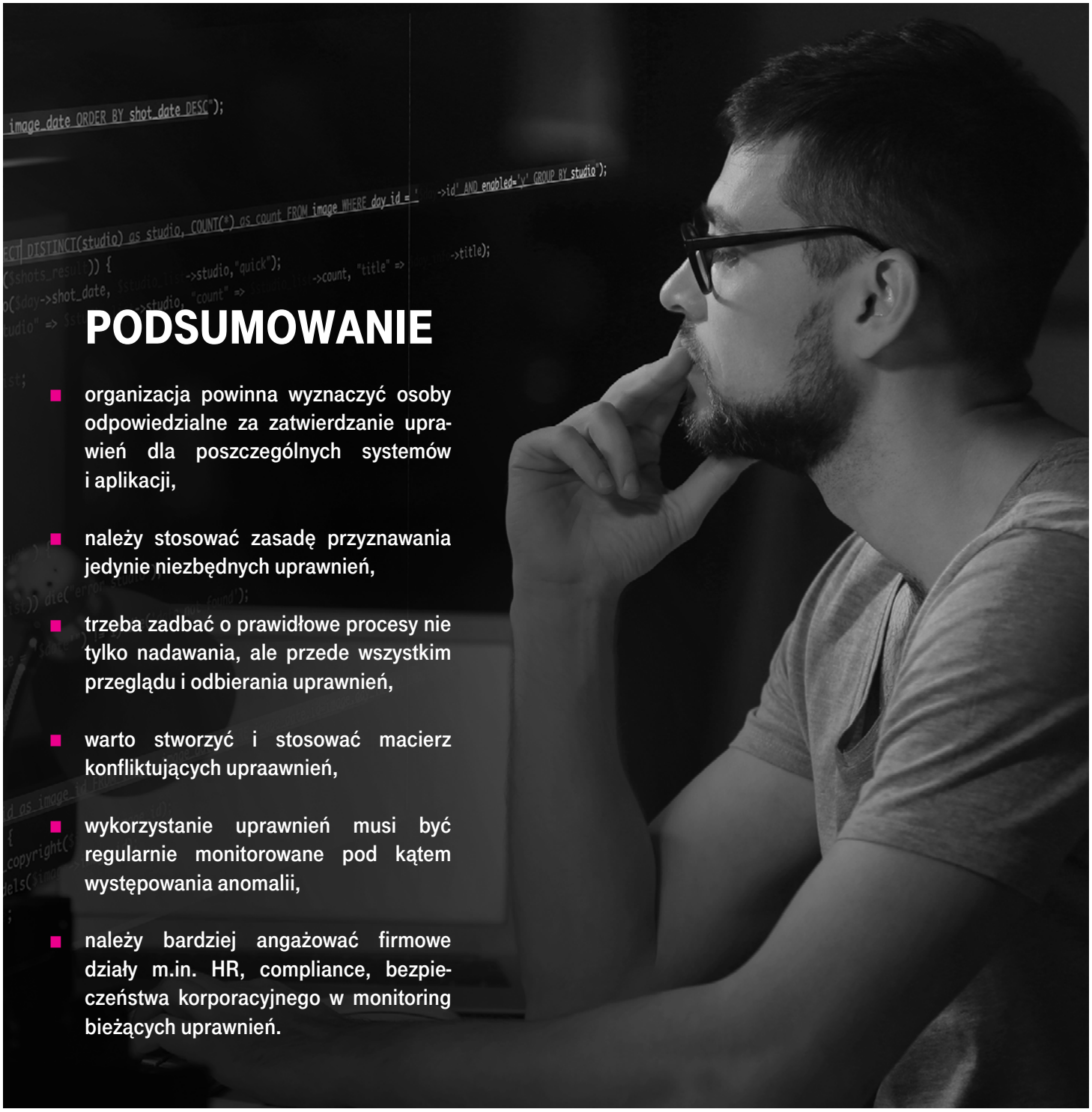
Oczywiście w zarządzaniu uprawnieniami mogą pomóc np. okresowe raporty wskazujące, kto jakimi uprawnieniami dysponuje w kontekście zajmowanego stanowiska. Proces identyfikacji nadmiarowych uprawnień można częściowo zautomatyzować, jednak niewiele jest organizacji, którym udało się zapewnić terminowe odbieranie uprawnień użytkownikom.

W zapewnieniu prawidłowej konfiguracji uprawnień w systemach na pewno pomoże sporządzenie macierzy konfliktujących uprawnień, czyli listy uprawnień, których nie powinna posiadać jedna i ta sama osoba. Sporządzenie takiej listy może być sporym wysiłkiem, jednak to bardzo przydatne narzędzie.

JAK MONITOROWAĆ

Trudno zapobiegać nadużyciom nie monitorując zagrożonych procesów. Na rynku istnieje wiele narzędzi wspierających zarządzanie uprawnieniami i ich wdrożenie może pomóc organizacji uporać się z takim problemem. Z jednej strony dzięki automatyzacji będzie można odciążyć administratorów, którzy będą mogli zająć się innymi zadaniami, a z drugiej pozwoli ona w większym stopniu na wyeliminowanie błędów w procesach nadawania i odbierania uprawnień oraz wykrywaniu uprawnień nadmiarowych.

Monitorowanie wykorzystania uprawnień, szczególnie w przypadku kont uprzywilejowanych, powinno być istotnym elementem usługi Security Operations Center. Prawidłowo skonfigurowane reguły monitoringu mogą pomóc wykryć zarówno uzyskiwanie uprawnień przez osoby nieautoryzowane, jak i nadużywanie posiadanych uprawnień przez osoby autoryzowane.



PODSUMOWANIE

- organizacja powinna wyznaczyć osoby odpowiedzialne za zatwierdzanie uprawień dla poszczególnych systemów i aplikacji,
- należy stosować zasadę przyznawania jedynie niezbędnych uprawnień,
- trzeba zadbać o prawidłowe procesy nie tylko nadawania, ale przede wszystkim przeglądu i odbierania uprawnień,
- warto stworzyć i stosować macierz konfliktujących upraawnień,
- wykorzystanie uprawnień musi być regularnie monitorowane pod kątem występowania anomalii,
- należy bardziej angażować firmowe działy m.in. HR, compliance, bezpieczeństwa korporacyjnego w monitoring bieżących uprawnień.

AKTUALIZACJE

Według badania przeprowadzonego niedawno przez Ponemon Research Institute aż w 57% włamań skutkujących wykradzeniem danych głównym sposobem przełamania zabezpieczeń było używanie przez ofiarę nieaktualnego oprogramowania ze znanymi podatnościami.[1] Atakujący nad wyraz rzadko używają błędów jeszcze nieujawnionych, ponieważ większość firm i organizacji nadal nie potrafi wystarczająco dobrze zarządzać aktualizacjami używanych systemów i aplikacji. Dlaczego jest to takie trudne zadanie i jak radzić sobie z tą kategorią problemów?

1. Jak ważne są regularne aktualizacje aplikacji webowych i systemów operacyjnych
2. O przypadkach cyberataków na największe światowe koncerny spowodowanych brakiem aktualizacji aplikacji lub systemu operacyjnego
3. Czy mechanizmy zabezpieczające aplikacje www przed znanymi i świeżo odkrytymi podatnościami mogą skutecznie zlikwidować podatności

AKTUALIZACJE APLIKACJI I ICH KOMPONENTÓW

Nie bez powodu „Używanie komponentów ze znanymi podatnościami" od lat ma stałe miejsce na liście 10 najczęściej występujących problemów z bezpieczeństwem aplikacji WWW, zwanej OWASP Top10. Choć w dzisiejszym świecie to właśnie aplikacje WWW odgrywają dominującą rolę, to problem aktualizacji dotyczy wszystkich rodzajów aplikacji używanych w firmach i instytucjach. Mnogość narzędzi, w które wyposażamy naszych pracowników i klientów powoduje, że coraz trudniej jest zachować nad nimi kontrolę. Już sama inwentaryzacja używanych rozwiązań dla wielu organizacji stanowi problem, a zbadanie stanu ich aktualizacji okazuje się wyzwaniem przerastającym większość firm. Dobrym przykładem, czym kończy się taka sytuacja, może być historia amerykańskiej firmy Equifax, z której włamywacze wykradali przez wiele miesięcy dane jej klientów. Gdy okazało się, że popularny komponent aplikacji Apache Struts posiada krytyczną podatność, umożliwiającą zdalne wykonanie kodu, pracownicy Equifaxu dwukrotnie skanowali swoją sieć w poszukiwaniu aplikacji podatnych na atak – i dwukrotnie ich nie wykryli. Okazało się jednak, że włamywacze byli sprawniejsi i między pierwszym a drugim skanowaniem zidentyfikowali podatny serwer, włamali się do niego i następnie miesiącami wyprowadzali cenne informacje z kilkudziesięciu baz danych.[2]

1 https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/analyst-report/ponemon-state-of-vulnerability-response.pdf
2 https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf

AKTUALIZACJE SYSTEMÓW OPERACYJNYCH

Oprócz aktualizacji aplikacji nie mniej ważnym problemem jest aktualizacja używanych systemów operacyjnych. Wagę tego zagadnienia najlepiej pokazał atak złośliwego oprogramowania WannaCry, które wykorzystywało podatność w usłudze SMB (Server Message Block) znaną w momencie ataku od kilku tygodni. Mimo iż istniały aktualizacje pozwalające na usunięcie podatności, WannaCry było w stanie zainfekować tysiące firm na całym świecie, w tym także wielkie korporacje takie jak Nissan, Renault czy FedEx[3] i poczynić w nich znaczne zniszczenia. Choć konieczność aktualizacji systemów Windows i waga podatności były świetnie znane, to nie wystarczyło to do zapewnienia, by publicznie dostępne serwery zostały załatane w ciągu miesiąca od opublikowania narzędzi umożliwiających przeprowadzenie ataku. Co więcej, ataki WannaCry zdarzają się nadal, nawet półtora roku od jego pojawienia się w sieci. Niedawno ich ofiarą padł producent układów scalonych używanych w produktach firmy Apple. Źródłem infekcji okazał się być laptop serwisanta, podłączony do wewnętrznej sieci produkcyjnej. Mimo skali zagrożenia komputery w niej obecne nie otrzymały na czas odpowiednich aktualizacji.

WYGRAĆ WYŚCIG

Walka z cyberprzestępcami nie jest prostym zadaniem. W opisywanym powyżej przypadku firmy Equifax między opublikowaniem informacji o odkryciu błędu a jego wykorzystaniem przez przestępców minęły zaledwie dwa dni. W przypadku występujących w ostatnich miesiącach podatności serwisów opartych o platformę Drupal czas od odkrycia do wykorzystania błędu skrócił się do kilku godzin. Przestępcy wiedzą, że czas na przeprowadzenie ataku na najciekawsze cele szybko upływa, dlatego na bieżąco monitorują nowe podatności i starają się je jak najszybciej wykorzystać. Organizacje, które chcą im stawić czoła, nie mogą być w tym wyścigu gorsze.

Nie każda firma może jednak utrzymywać całodobowy zespół monitorowania i reagowania na tego typu incydenty. Z pomocą przychodzą tu usługi oferowane i zarządzane przez zewnętrzne podmioty takie jak np. Managed Web Application Firewall, czyli mechanizmy zabezpieczające aplikacje WWW przed znanymi i świeżo odkrytymi podatnościami. Dzięki pracy ekspertów dbających o aktualizacje sygnatur ataków firmy mogą stosować „wirtualne likwidowanie podatności" – zanim zdążą zaktualizować swoje aplikacje, odpowiednie platformy uniemożliwią przestępcom wykorzystanie błędów.

ZŁOŚLIWE AKTUALIZACJE

Omawiając temat aktualizacji oprogramowania nie sposób nie wspomnieć o atakach, w których wektorem ataku były złośliwe, zmodyfikowane przez przestępców aktualizacje oprogramowania używanego przez wiele firm na całym świecie. Takimi przykładami mogą być niedawne incydenty NotPetya czy CCleanera, gdzie dzięki przejęciu kontroli nad serwerem aktualizacji przestępcy mogli w niezauważalny dla użytkowników sposób infekować miliony komputerów. Te ataki mogą stanowić istotne zagrożenie i być argumentem przeciwko regularnemu aktualizowaniu aplikacji. Należy jednak zauważyć, że ryzyka, wynikające z używania nieaktualnych aplikacji, znacznie przewyższają te płynące z ich regularnego aktualizowania. Ataki na nieaktualne aplikacje trudno nawet zliczyć, podczas gdy ataki złośliwych aktualizacji to nadal pojedyncze incydenty w skali roku.

3 https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

PODSUMOWANIE

Dbanie o terminowe aktualizacje jest trudnym, nigdy nie kończącym się wyzwaniem. Aby mu podołać warto przestrzegać poniższych zaleceń:

- **Inwentaryzacja wszystkich wykorzystywanych systemów i aplikacji oraz skanowanie wykorzystywanych aplikacji pod kątem ich podatności.**
- **Usuwanie nieużywanych systemów i aplikacji pozwala zmniejszyć pulę rozwiązań wymagających aktualizacji.**
- **Automatyzacja procesów aktualizacji jest przydatna w organizacji o każdej skali działania i znacząco odciąża pracowników odpowiedzialnych za ten proces, pozwalając im skupić się na aplikacjach i systemach, gdzie automatyzacja aktualizacji nie jest pożądana lub możliwa.**
- **W przypadkach, gdy aktualizacja nie jest możliwa, należy wdrożyć inne mechanizmy, takie jak filtrowanie ruchu, separacja podatnych systemów oraz monitoring.**

ATAKI UKIERUNKOWANE

Administratorzy systemów jako osoby o ponadprzeciętnej wiedzy na temat ataków na użytkowników często ostrzegają przed nimi swoich mniej świadomych współpracowników. Rzadko jednak zdają sobie sprawę z tego, że sami mogą paść ofiarą ataków precyzyjnie wymierzonych właśnie w nich. Tymczasem to właśnie administratorzy stanowią niezwykle atrakcyjny cel dla cyberprzestępców – przejmując kontrolę nad ich stacją roboczą czy kontem można zdobyć dostęp do znacznie cenniejszych zasobów. Jak zatem są atakowani administratorzy i jak mogą się przed tym bronić?

1. Dlaczego administratorzy są atrakcyjnym celem dla cyberprzestępców
2. W jaki sposób najczęściej atakowani są administtratorzy
3. Co może pomóc w minimalizacji skutków cyberataków na administratorów

! ATAKI UKIERUNKOWANE

Jednym z najlepszych przykładów tego, co może spotkać administratorów firmowych systemów, jest historia ataku na firmę Bitstamp, prowadzącą jedną z największych giełd kryptowalut.[1] W wyniku skutecznych działań przestępców giełda straciła 18 000 bitcoinów, w momencie kradzieży wartych ponad 5 milionów dolarów. Cyberprzestępcy bardzo drobiazgowo przygotowali się do ataku i na długo przed nim przeprowadzili dokładną inwigilację pracowników firmy, czego efektem było poddanie ich próbom infekcji. I tak miłośnik muzyki typu punk rock otrzymał zaproszenie na festiwal, na którym miały zagrać jego ulubione zespoły. Prezes firmy, który kiedyś pracował jako dziennikarz, dostał do recenzji artykuł prasowy, poświęcony interesującej go tematyce. Z kolei pracownik, który krótko przed atakiem odszedł z innej firmy, by pracować w Bitstampie, został poproszony o wypełnienie ankiety dotyczącej poprzedniego pracodawcy. Mimo przejęcia kontroli nad kilkoma firmowymi komputerami przestępcy nie uzyskali jednak dostępu do głównego portfela firmy. Dopiero skuteczny atak na głównego administratora, który otrzymał zaproszenie do prestiżowego stowarzyszenia branżowego, pozwolił napastnikom na kradzież pieniędzy. W każdym przypadku ataki trwały wiele dni i polegały zarówno na konwersacjach na Skype, jak i wymianie poczty elektronicznej. Jak widać na powyższym przykładzie skuteczne przeciwstawienie się zdeterminowanemu napastnikowi nie jest łatwym zadaniem. Nawet dla doświadczonych administratorów.

1 https://www.docdroid.net/159hk/270137312-bitstamp-incident-report-2-20-15.pdf

ILE KOSZTUJE ATAK

Choć w przypadku ataków socjotechnicznych trudno znaleźć dobry punkt odniesienia, to ataki na systemy operacyjne i aplikacje można dość prosto porównać. Dobrym przykładem może być tutaj cennik firmy Zerodium, która skupuje różne metody ataków (później je odsprzedając z odpowiednią marżą) i publikuje w sieci swoje cenniki.[2] Ataki na domowe routery czy popularne fora internetowe kosztują 10 tysięcy dolarów. Skuteczne ataki na Adobe Readera, Safari czy Firefoxa to koszt już 80 tysięcy dolarów, podczas kiedy możliwość wykonania dowolnego kodu na najnowszym iPhonie bez udziału użytkownika kosztować będzie aż półtora miliona dolarów. Podobny atak na platformę Windows przyniesie jego odkrywcy pół miliona dolarów.

AKTUALIZACJE OPROGRAMOWANIA

Czasem ataki wymierzone w administratorów są nad wyraz trudne do wykrycia i mogą przyjmować postać złośliwej aktualizacji oprogramowania. Tak było w przypadku narzędzia XManager, służącego do zarządzania serwerami.[3] Przestępcy przejęli kontrolę nad infrastrukturą producenta tej aplikacji i dodali swój własny kod do kolejnej jej wersji. Głównym zadaniem złośliwego oprogramowania było informowanie jego autorów o udanej infekcji oraz zbieranie informacji o zarażonym środowisku. Z uwagi na fakt, że było to narzędzie administracyjne, działało zawsze z wysokimi uprawnieniami, pozwalając przestępcom na sprawną realizację ich celów.

Innym podobnym przypadkiem była infekcja oprogramowania EvLog, używanego przez administratorów do analizy logów systemowych. W tym incydencie skutecznie zainfekowane zostały dziesiątki firm i organizacji z całego świata, a przestępcy uzyskali dostęp do interesujących ich uprawnień.[4] Tego rodzaju ataki są szczególnie niebezpieczne, ponieważ pozostawiają niewiele śladów w systemach ofiary. Ich wykrycie możliwe jest najczęściej tylko dzięki wnikliwemu monitorowaniu ruchu sieciowego zarażonej organizacji.

ZARZĄDZANIE UPRAWNIENIAMI

Warto pamiętać, że im prostsza i łatwiejsza jest praca administratora, tym prostsze będzie zadanie potencjalnego włamywacza. Administratorzy, korzystający z jednego konta z wysokimi uprawnieniami do wszystkich swoich zadań, bardzo ułatwiają pracę atakującym. Wystarczy, że napastnik uzyska dostęp do dowolnego komputera, na którym wcześniej logował się administrator (a komputer nie został od tamtej pory ponownie uruchomiony) i nawet z poziomu zwykłego użytkownika będzie mógł próbować odczytać z pamięci komputera poświadczenia administratora. Służy do tego bardzo skuteczne narzędzie Mimikatz, używane regularnie zarówno przez pentesterów jak i włamywaczy. Ryzyko takiego ataku ograniczyć może używanie różnych kont do różnych celów.

Czynności administratora serwera nie zawsze wymagają uprawnień administratora domeny, a sporą część pracy administrator może wykonać z uprawnieniami zwykłego użytkownika. Warto zadbać o to, by poziom używanych uprawnień był zawsze proporcjonalny do wykonywanych zadań – utrzymywanie takiej higieny pracy znacząco skomplikuje życie potencjalnego napastnika. Należy także pamiętać o monitorowaniu wszystkich czynności wykonywanych przez administratorów. Ich rejestrowanie powinno przebiegać w taki sposób, by sami administratorzy nie mogli modyfikować tych zapisów. Warto także wprowadzić mechanizmy wykrywania i analizy ewentualnych anomalii, takich jak chociażby logowania poza tradycyjnymi godzinami pracy. W realizacji tych zadań bez dodatkowego obciążania istniejącego zespołu może pomóc zewnętrzna usługa SOC.

2 https://www.zerodium.com/program.html
3 https://securelist.com/shadowpad-in-corporate-networks/81432/
4 http://blog.comsecglobal.com/2017/03/kingslayer-supply-chain-attack.html

PODSUMOWANIE

Administratorzy stanowią bardzo atrakcyjny cel dla przestępców. W dbaniu o właściwy poziom bezpieczeństwa ich pracy pomoże przestrzeganie poniższych zaleceń:

- **Administrator musi zdawać sobie sprawę, że on sam także może paść ofiarą ataku wycelowanego**
- **Praca z najniższymi możliwymi w danym momencie uprawnieniami pomaga w minimalizacji skutków udanego ataku**
- **Niezbędne jest rejestrowanie i monitorowanie działań administracyjnych**
- **W wykrywaniu incydentów pomóc może monitoring anomalii.**

Poznaj usługi bezpieczeństwa IT od T-Mobile:
https://biznes.t-mobile.pl/pl/produkty-i-uslugi/cyberbezpieczenstwo-i-ochrona