Microsoft

Odpowiedzialna cyfryzacja polskich uczelni.

O bezpiecznej społeczności akademickiej w wirtualnej przestrzeni.

ZARZĄDZANIE
I REKOMENDACJE:

- zabezpieczenia i komunikacja
- tożsamość i dostępy
- urządzenia
- ryzyko
- zagrożenia

DRUGIE WYDANIE

Szanowni Państwo,

prezentujemy drugie wydanie publikacji, która zawiera najistotniejsze kwestie bezpiecznej i odpowiedzialnej cyfryzacji uczelni. Została ona przygotowana w ramach projektu „Uczelnia w Chmurze Microsoft". Zebrane informacje po raz kolejny są oparte na międzynarodowym i krajowym doświadczeniu firmy Microsoft na rynku edukacyjnym. Autorzy tekstu wskazali najczęściej przeprowadzane cyberataki na polskie szkoły wyższe, aby w czytelny i zrozumiały sposób zaprezentować pigułkę wiedzy o cyberbezpieczeństwie społeczności akademickiej. Jej drugie wydanie uwzględnia najbardziej aktualne kwestie branży technologicznej w obszarach technicznych i zarządczych, m.in. w obliczu hybrydowego wymiaru wojny na Ukrainie.

Rozwiązania problemu cyberbezpieczeństwa uczelni wykraczają poza środki techniczne. Eksperci szkolnictwa wyższego, którzy brali udział w konsultacjach treści obydwu wersji publikacji, rekomendują dodatkowe działania organizacyjne niewymagające nakładów finansowych. W drugim, poniższym wydaniu zaktualizowaliśmy ich zbiór. Zespół Microsoft dla Edukacji dysponuje doświadczeniem opartym na współpracy z polskimi i zagranicznymi szkołami wyższymi: władzami uczelni, ekspertami ds. IT oraz partnerami technologicznymi. Zapraszamy do kontaktu i stałej współpracy dotyczącej doradztwa i wdrożenia odpowiednich środków technicznych i organizacyjnych na Państwa Uczelni. Możliwość konsultacji pod adresem: edukacja@microsoft.com.

Zespół Microsoft dla Edukacji

AUTOR

Sebastian Pawłowski
certyfikowany trener Microsoft

Zajmuje się cyberbezpieczeństwem i wdrażaniem technologii zabezpieczeń w usługach Microsoft 365. Od 20 lat związany z branżą IT. Założył specjalistyczną firmę RedFlag.tech, która pomaga przedsiębiorstwom i organizacjom pracować w bezpieczniejszym świecie. Zdobył certyfikaty: Enterprise Administrator Expert, Security Administrator Associate i Modern Desktop Administrator Associate

RECENZENCI

prof. dr hab.
Tomasz Szapiro

Magisterium z fizyki (UW), doktorat z matematyki (PAN), habilitacja (SGH) i tytuł profesora z ekonomii. Pracuje w SGH, rektor tej uczelni w kadencji 2012-2016. Zajmuje się metodami wspomagania i analizy decyzji w ekonomii oraz zarządzaniu. Autor i współautor sześciu książek, współredaktor rocznika „Annals of Operations Research", napisał ponad 100 artykułów i prac konferencyjnych

Barbara Michalska
dyrektorka ds. rynku edukacyjnego Microsoft Polska

Absolwentka Politechniki Warszawskiej, Wydziału Matematyki i Nauk Informacyjnych oraz SGH. Entuzjastka wszelkich innowacji, które czynią nasz świat miejscem lepszym do życia, a naukę – prostszą i bezpieczną. Wierzy, że dzięki zastosowaniu technologii i cyfrowych rozwiązań uda nam się wspomagać uczenie, budować nowe kompetencje i przygotować uczniów do wykonywania zawodów przyszłości

WPROWADZENIE

Liderzy nauki i szkolnictwa wyższego zdążyli się dostosować do modelu kształcenia i zarządzania uczelnią w sposób hybrydowy. Nadali oni procesowi cyfryzacji odpowiednio szybkie tempo, analizując przy tym czynniki, które zagrażają społeczności akademickiej w trakcie korzystania z najnowszych technologii. Zapewnienie wirtualnego bezpieczeństwa jest równie istotną kwestią co dopasowanie i wdrożenie skutecznego cyfrowego systemu zarządzania procesami dydaktycznymi, naukowymi i administracyjnymi. **Edukacja to najbardziej narażony na cyberataki sektor. Według raportu „Global threat activity" prowadzonego przez Microsoft 80% zgłoszonych przypadków złośliwego oprogramowania1 pochodzi z instytucji i placówek edukacji.**

Cyberprzestępcy stale pracują nad udoskonalaniem swoich metod i dostosowują je do zmieniających się warunków, przez co liczba zagrożeń nieustannie rośnie. **W raporcie „Digital Defence Report 2022" Microsoft prezentuje m.in. hybrydowy wymiar zbrojnej napaści na Ukrainę, wskazując 237 cyberataków przeprowadzonych przeciwko Ukrainie podczas pierwszych 6 tygodni inwazji.** Władze uczelni już teraz muszą uwzględniać w swoich działaniach i etyce zarządzania wirtualne bezpieczeństwo każdej osoby w ich społeczności: kandydatów, studentów, doktorantów, nauczycieli akademickich oraz pracowników administracyjnych. Tylko takie podejście zagwarantuje obecnie odpowiedni poziom ochrony.

Spełniając standardy wyznaczone przez europejskie i państwowe instytucje akredytujące, należy tworzyć system, którego jakość będzie wyznaczana również przez wirtualne bezpieczeństwo społeczności akademickiej. Jest ono nieodłącznym elementem metod i technik kształcenia na odległość, procesów badawczych oraz administracyjnych.

[1]Na podstawie zgłoszonych przypadków złośliwego oprogramowania w ciągu ostatnich 30 dni. Dane na 20 stycznia 2023 r. Raport dostępny na stronie: wwwm.microsoft.com/en-us/wdsi/threats.

SPIS TREŚCI

Cyberataki na polskiej uczelni

2

Nieodpowiednie zabezpieczenie urządzeń pracowników

PRZYCZYNA
Korzystanie z prywatnych urządzeń w pracy, które nie gwarantują odpowiedniego stopnia zabezpieczenia.

EFEKT
Dane urządzenie jest furtką, która umożliwia złym podmiotom dostęp do środowiska uczelni oraz danych osobowych.

ROZWIĄZANIE
Centralne zarządzanie urządzeniami pracowników z najwyższymi standardami bezpieczeństwa.

Nieprzygotowanie na ataki ransomware

PRZYCZYNA
To atak polegający na zablokowania dostępu do infrastruktury w celu wyłudzenia okupu. Podwodem mogą być nieprawidłowe zabezpieczenie i brak monitorowania zagrożeń na serwerach lokalnych.

EFEKT
Utrata dostępu do narzędzi, danych i całej infrastruktury uczelni, potrzeba opłacenia wysokiego okupu z brakiem gwarancji.

ROZWIĄZANIE
Ciągły monitoring wydarzeń w środowisku i możliwych zagrożeń, utworzenie i prowadzenie kopii zapasowej całego środowiska, która umożliwi przywrócenie dostępu.

Ataki phishingowe

PRZYCZYNA
Podszywanie się złych podmiotów pod tożsamość innych osób lub jednostek.

EFEKT
Wyłudzenie informacji i uzyskanie dostępu do środowiska uczelni.

ROZWIĄZANIE
Ochrona antyspamowa, weryfikacja linków oraz załączników w poczcie, poprawienie wiedzy i świadomości wśród pracowników, wykładowców i studentów.

Nieprawidłowe zarządzanie danymi i brak ich zabezpieczenia w sieci

PRZYCZYNA
Nieodpowiednie przechowywanie danych na lokalnych serwerach, których zabezpieczenie (fizyczne i cyfrowe) jest bardzo ograniczone.

EFEKT
Wycieki danych osobowych, spadek zaufania społeczności, kary finansowe.

ROZWIĄZANIE
Przechowywanie i zarządzanie danymi w chmurze zgodnie z najwyższymi standardami polityk prywatności. Wprowadzenie polityki Zero Trust.

3 Bezpieczne zarządzanie uczelnią w pigułce

ZASADA OGRANICZONEGO ZAUFANIA

Procedury pozwalają dochować należytej staranności. Jednak procedury bez wsparcia technologii to ochrona iluzoryczna. Jest oczywiste, że uczelnia powinna dysponować sformalizowanymi zasadami dotyczącymi np. polityk resetu haseł, cyklicznej kontroli dostępu, standardów aktualizacji oprogramowania, korzystania z urządzeń mobilnych w dostępie do danych organizacji. Jednak biorąc pod uwagę skalę działania organizacji, jaką jest uczelnia, tylko procedury oparte na technologii mogą sprawdzić każde żądanie dostępu i w zależności od parametrów logowania zezwolić, zablokować lub wymusić dodatkową weryfikację.

Organizacja składająca się z 5000 użytkowników generuje około 245 000 czynności uwierzytelniania tygodniowo. Szanse wyodrębnienia zdarzeń podejrzanych bez użycia zasad zautomatyzowanych są znikome. Dlatego do skutecznego zabezpieczenia wymagana jest technologia adekwatna do potencjalnego ryzyka.

Nie wszyscy użytkownicy w organizacji są tak samo wartościowi dla potencjalnych atakujących. Dobrą praktyką jest podział na grupy i zastosowanie technologii współmiernych do ich potencjału ryzyka. Błędem jest jednak całkowite pomijanie w stosowaniu ochrony grup niskiego zaufania. To na przykład pracownicy uczelni funkcjonujący w strukturach tylko przez określony czas, poza regularnymi zasadami zatrudnienia, a mający dostęp do potencjalnie wartościowych informacji. Im mniejsze zaufanie, tym mocniejsza ochrona technologiczna powinna być zastosowana.

Zero Trust

Rekomendowanym modelem tworzenia środowiska odpornego na współczesne zagrożenia jest koncepcja Ograniczonego Zaufania, czyli *Zero Trust Security*. W tym modelu przyjmuje się założenie, że każde zabezpieczenie może zostać naruszone. Oznacza to, że nic nie jest bezpieczne *a priori*. Dlatego podstawą jest weryfikacja każdego żądania dostępu w taki sposób, jakby pochodziło z niekontrolowanej sieci i stanowiło potencjalne zagrożenie. Niezależnie od tego, skąd pochodzi żądanie i jakiego zasobu dotyczy. Pojęcie zasobu należy traktować w sposób szeroki, czyli jako dane, aplikacje, urządzenia i inne miejsca lub sposoby przetwarzania informacji. Model *Zero Trust* wymaga, aby „nigdy nie ufać i zawsze weryfikować". Dostęp do zasobów jest określany przez dynamiczne zasady – w tym bieżący stan tożsamości użytkownika, kanał dostępu do usługi, stan urządzenia, z którego pochodzi żądanie, położenie geograficzne – i może obejmować inne atrybuty behawioralne.

Trzy podstawowe zasady *Zero Trust*, to:

- **Każdorazowa weryfikacja**
- **Korzystanie z dostępu z najniższym możliwym poziomem uprawnień**
- **Założenie, że bezpieczeństwo mogło zostać naruszone.**

Microsoft stosuje z powodzeniem to podejście i pomaga organizacjom we wdrożeniach opartych na metodzie *Zero Trust*. Większość strategii zabezpieczeń opisanych w niniejszej publikacji realizuje w praktyce koncepcję Ograniczonego Zaufania.

ZABEZPIECZENIA KOMUNIKACJI

Poczta

Poczta elektroniczna jest najczęściej wykorzystywaną usługą informatyczną i najpopularniejszą usługą chmurową. Możliwość korzystania z dowolnego miejsca i na dowolnym urządzeniu jest tak samo atrakcyjna dla użytkownika, jak i dla

potencjalnych atakujących. Systemy pocztowe korzystające z logowania wyłącznie przy użyciu hasła należy uznać za niebezpieczne. Największa liczba ataków, według danych prezentowanych przez Microsoft, przebiega z wykorzystaniem podstawowych protokołów uwierzytelniania – czyli gdy do uwierzytelnienia stosowane są wyłącznie nazwa użytkownika i jego hasło.

Microsoft rekomenduje przejście na pocztę umożliwiającą logowanie wieloskładnikowe. Hasło może zostać ujawnione i wykorzystane bez naszej zgody. Wszyscy znamy przykłady tego typu nadużyć. Dodatkowy składnik logowania, np. zatwierdzenie specjalnego powiadomienia w aplikacji mobilnej, chroni nas przed nieautoryzowanym logowaniem z użyciem wykradzionego hasła. Uczelnie nie powinny już akceptować standardów poczty opartych na uwierzytelnianiu starszego typu. Podstawowe protokoły uwierzytelniania takie jak IMAP/POP/SMTP powinny być zablokowane lub

przynajmniej ograniczone do niezbędnego minimum.

Jeśli to możliwe, stosujmy jeden spójny system autoryzacji użytkowników. W usługach Microsoft 365 każdy użytkownik posiada jeden login i jedno hasło do wszystkich usług w chmurze a uwierzytelnienie przebiega na jednej platformie zarządzania tożsamością. Dzięki temu logując się do poczty elektronicznej, Teams, OneDrive czy do urządzenia Windows 10/11 korzystamy z tego samego loginu i tego samego systemu uwierzytelniania. Ochrona tożsamości cyfrowej użytkownika sprowadza się wówczas do zabezpieczenia jednego centralnego systemu.

Korzystanie z prywatnych adresów e-mail w korespondencji służbowej (w tym z serwisów konsumenckich, tj. Gmail.com, Outlook.com, Onet.pl, Wp.pl, Interia.pl) powinno być uregulowane proceduralnie. Dla korespondencji poufnej należy dodatkowo stosować łatwą w użyciu technologię ochrony i szyfrowania informacji, której opis działania znajduje się w dalszej części publikacji.

Załączniki

Najczęstszą drogą dostarczenia złośliwego oprogramowania jest e-mail. Załącznik podający się za dokument PDF po otwarciu okazuje się złośliwym oprogramowaniem np. typu *ransomware*. Jest to kod wykonywalny, który szyfruje dane w celu uzyskania okupu podczas cyberataku.

Jak sprawdzić prawdziwość załącznika? Nie ma innego sposobu, trzeba go otworzyć. Jednak nie przez użytkownika, a przez technologię detonacji, która działa, zanim załącznik trafi do skrzynki odbiorczej. Plik otwierany jest w zabezpieczonym, zwirtualizowanym środowisku, w pełni odizolowanym od komputera użytkownika. Dostarczenie załącznika nastąpi tylko wtedy, gdy jego detonacja (otwarcie) nie wywoła nieprzewidzianych skutków. Funkcje takie jak Safe Attachments oraz Safe Links w Microsoft Defender for Office 365 pozwalają chronić uczelnię przed ransomware – oprogramowaniem szyfrującym dla uzyskania okupu podczas cyberataku. Działa to również w przypadku plików przekazywanych do Teams, SharePoint czy OneDrive oraz wszystkich odnośników klikanych w tych usługach przez użytkowników. Tradycyjna metoda ochrony poczty elektronicznej polegająca na filtrowaniu załączników w oparciu o rodzaj pliku, nie zapewnia dziś wystarczającego poziomu bezpieczeństwa.

Konfiguracja

Zalecenia dotyczące konfiguracji usług zmieniają się regularnie w miarę rosnących zagrożeń. Należy regularnie audytować stosowane zabezpieczenia i aktualizować je zgodnie z rekomendacjami dostawcy usługi lub zaleceniami instytucji zajmujących się cyberbezpieczeństwem.

Najczęstszym błędem jest pozostawienie ustawień domyślnych, zwłaszcza przy korzystaniu z usług chmurowych. Na przykład w ustawieniach bazowych dla Microsoft Azure Active Directory użytkownicy niebędący administratorami mogą samodzielnie

[2] Ransomware – oprogramowanie szyfrujące dla okupu.

udzielać zgody na rejestrację aplikacji chmurowych korzystających z podstawowych danych katalogu Azure AD, takich jak nazwa użytkownika. W większości przypadków należy te uprawnienia wyłączyć i korzystać z procesu akceptacji, który angażuje dedykowanych administratorów.

Innym przykładem przestarzałych ustawień mogą być zasady dotyczące wygasania haseł. Microsoft od kilku lat rekomenduje, aby hasła nie wygasały. Jednak nie może tego zmienić automatycznie, na poziomie platformy, dla usług zakupionych i konfigurowanych kilka lat temu. Periodyczna zmiana hasła prowadzi do korzystania przez użytkowników ze schematów, które są łatwe do odgadnięcia i nie stanowią dobrego zabezpieczenia. Należy zrewidować własne praktyki w tym zakresie.

Inaczej jest w przypadku przeglądu metod używanych jako dodatkowy element uwierzytelnienia. Użytkownicy powinni periodycznie kontrolować metody logowania zarejestrowane na swoim koncie.

Przeglądarka w usługach opartych na chmurze jest podstawowym kanałem dostępu. Dostawcy usług koncentrują się najczęściej na wygodzie użytkowania, nie zawsze właściwie oceniając ryzyko. Korzystanie z domyślnych zasad dla sesji przeglądarkowych może być niebezpieczne. Należy przeanalizować zasady dotyczące częstotliwości logowania i trwałości sesji przeglądarki, zwłaszcza przy dostępie z prywatnych urządzeń użytkowników.

Częstotliwość logowania w przeglądarce to czas, jaki upływa od interaktywnego logowania do automatycznego wylogowania. Aby zmniejszyć ryzyko kradzieży poświadczeń podczas sesji użytkownika, zaleca się ograniczenie tego czasu do uniwersalnego interwału 12 godzin. Natomiast trwała sesja przeglądarki to funkcja, która pozwala na pozostanie zalogowanym nawet po zamknięciu okna przeglądarki. Sesje przeglądarki nie powinny być trwałe – a właśnie takie są standardowe ustawienia w wielu usługach chmurowych. Należy ograniczać ryzyko kradzieży poświadczeń podczas korzystania z przeglądarki i wyłączyć trwałe sesje.

ZABEZPIECZENIE TOŻSAMOŚCI

Uwierzytelnianie wieloskładnikowe

Dziś login i hasło to zdecydowanie za mało. Taka metoda weryfikacji tożsamości użytkownika jest traktowana jako niespełnienie wymagań technicznych adekwatnych do ryzyka. Jesteśmy zgodni, że użytkownicy potrzebują łatwego dostępu do aplikacji i danych, jednak samo hasło nie zabezpiecza uczelni w wystarczający sposób. Bezwarunkowo należy stosować uwierzytelnianie wieloskładnikowe.

Co to znaczy? Proces logowania powinien angażować nie tylko to, co znamy (czyli hasło), lecz także coś, co mamy, np. telefon komórkowy lub sprzętowy klucz zabezpieczeń. Dzięki temu poznanie naszego hasła przez wyciek lub ujawnienie nie pozwoli na skuteczne uzyskanie dostępu.

Do poprawnego uwierzytelnienia wymagane jest najczęściej przepisanie kodu otrzymanego w wiadomości SMS lub zatwierdzenie powiadomienia w aplikacji mobilnej. Ponieważ większość użytkowników ma telefon komórkowy, taka metoda uwierzytelniania jest łatwo dostępna dla każdej uczelni. Samoobsługowa rejestracja dodatkowego składnika logowania powinna być standardem przy pierwszym logowaniu do systemu uczelni. Uwierzytelnianie wielkoskładnikowe powinno obowiązywać wszystkich użytkowników bez wyjątku.

Jednak i w tym zakresie zalecenia dotyczące bezpieczeństwa cyfrowego ciągle ewoluują. Kod SMS nie jest uważany za wystarczająco bezpieczny, ze względu na uzależnienie od przestarzałej infrastruktury telekomunikacyjnej. Z kolei proste zatwierdzenie powiadomienia w aplikacji mobilnej – czyli stuknięcie w pojawiające się na ekranie telefonu powiadomienie – może prowadzić do przypadkowego logowania. Obydwie metody uznawane są już za nieodporne na ataki po-

legające na wyłudzaniu informacji (phishing) oraz ataki nękające użytkownika wielokrotnymi powiadomieniami. Dlatego należy zastąpić je lepszymi odpowiednikami.

Uczelnie powinny rezygnować z korzystania z wiadomości SMS jako metody uwierzytelniania wieloskładnikowego i zastępować SMS bezpieczniejszymi rozwiązaniami.

Za metody odporne na wyłudzenia (phishing) uznaje się dziś logowanie prowadzone całkowicie bez użycia hasła. Można skorzystać ze sprzętowego klucza zabezpieczeń FIDO2 lub logowania opartego na certyfikatach (CBA). Dopuszcza się uwierzytelnienie polegające na zatwierdzeniu powiadomienia w aplikacji mobilnej, któremu zawsze towarzyszy konieczność manualnego przepisania numeru z ekranu logowania. Określane jest to jako zatwierdzenie z „weryfikacją zgodnością numerów". Numer przepisany do powiadomienia w aplikacji musi być zgodny z numerem prezentowanym na ekranie logowania. Tego typu powiadomienie może dostarczać dodatkowych informacji kontekstowych, np. do jakiej aplikacji oraz z jakiego miejsca wskazanego na mapie wywołane zostało logowanie.

Te metody nie pozwolą na przypadkowe zatwierdzenie, czyli są odporne lub w miarę odporne na ataki wyłudzające. Jeśli nie znamy numeru wyświetlonego na ekranie logowania, bo nie my wyzwoliliśmy to logowanie, to nie zatwierdzimy przypadkowo otrzymanego powiadomienia.

Metodą alternatywną jest korzystanie z kluczy zabezpieczeń FIDO2. Posiadanie klucza (przedmiotu), PIN do klucza oraz przepływ elektromagnetyczny wywołany przez dotknięcie klucza całkowicie zastępują logowanie hasłem do usług chmurowych przez przeglądarkę lub do Windows na komputerze zarządzanym przez Azure AD. Konieczność dotknięcia klucza eliminuje możliwości nadużyć i logowania realizowanego przez boty. Ta metoda uznawana jest za jedną z bezpieczniejszych i nie angażuje dużych środków wymaganych na zakup i wdrożenie.

Użytkownicy rejestrują klucz samodzielnie, co oznacza, że nie wykorzystują zasobów uczelni do konfiguracji tej metody uwierzytelnienia. Dostęp do portalu samoobsługowego możliwy jest przez kod tymczasowy działający przez maksymalnie 8 godzin od wyznaczonej daty i godziny, który zaspokoi wymaganie weryfikacji wieloetapowej. Można dodatkowo ograniczyć lokalizację rejestracji klucza do IP uczelni lub lokalizacji zgodnej z IP obszaru geograficznego danego kraju (co jest zabezpieczeniem typu best effort – czyli możliwym do obejścia, chociażby przez wykorzystanie VPN).

Użytkownik nie ma hasła, więc go nie ujawni. Utrata PIN-u powoduje natomiast konieczność całkowitego resetu klucza.

Czynnikiem kosztotwórczym dla uczelni może być resetowanie haseł dla użytkowników. Stosując uwierzytelnianie wieloskładnikowe, możemy zezwolić na samodzielny reset hasła, którego użytkownik nie pamięta. W tym wypadku tożsamość użytkownika potwierdzi nie pracownik działu informatyki, tylko dodatkowe urządzenie (aplikacja i kod SMS jednocześnie). Należy stosować więcej niż jedną wymaganą metodę weryfikacji tożsamości, czyli np. powiadomienie w aplikacji z opcją zgodności numerów oraz dodatkowo kod SMS (kodu nie stosujemy do potwierdzania logowania!). Jest to rekomendowana przez Microsoft metoda weryfikacji przy samodzielnym resecie hasła. Najprostsze subskrypcje Microsoft nie dają jednak takiej możliwości.

ZABEZPIECZENIA DOSTĘPU

Dostęp warunkowy

Podstawowym założeniem metodyki opartej na Ograniczonym Zaufaniu (*Zero Trust*) jest kontrola każdej próby dostępu i jej ocena oparta na przyjętych zasadach.

Uczelnia może zezwolić na dostęp do krytycznych zasobów tylko z określonego adresu IP lub zablokować dostęp z obszarów geograficznych, z których zazwyczaj nikt nie

powinien się logować. Autentyczność położenia geograficznego może zostać przekazana przez aplikację uwierzytelniania na telefonie użytkownika. Jest to dość trudne do obejścia.

Inny przykład kontroli to wymaganie korzystania z urządzenia zarządzanego (znanego w IT uczelni) lub przynajmniej zarejestrowanego (to niższe i dające mniejsze możliwości zabezpieczenie). Próba dostępu z innego typu urządzenia może wiązać się z ograniczeniami dla użytkownika, np. załączników i dokumentów nie będzie można pobrać, wydrukować albo skopiować ich treści w przeglądarce.

Możemy blokować całkowicie korzystanie z aplikacji lub kontrolować tylko kanały dostępu do aplikacji, np. blokować dostęp przez przeglądarkę, aplikację mobilną lub program instalowany na komputerze czy tablecie. Można stosować warunki na podstawie typu urządzenia, np. komputery i telefony zarządzane otrzymają dostęp, urządzenia niezarządzane zostaną zablokowane. Analogicznie tworzymy zasady dostępu warunkowego dla systemów operacyjnych lub w dowolnych innych kombinacjach wszystkich dostępnych parametrów.

Absolutnie podstawowym wykorzystaniem technologii Dostępu Warunkowego jest wymaganie stosowania potwierdzenia logowania (MFA) dla wszystkich użytkowników oraz wyłączenie stosowania prostych protokołów uwierzytelniania np. dla poczty. Daje to pewność, że każdy obecny i przyszły użytkownik systemu uczelni będzie podlegał tym samym zasadom. A zasada nie będzie zależna od manualnej czynności administratora koniecznej do wykonania przy zakładaniu nowego konta użytkownika (odporność na błędy ludzkie). Daje to również pewność, że każdy kto przestał być pracownikiem lub studentem, nie otrzyma dostępu do zasobów, które od pewnego momentu mają być dla niego niedostępne.

Usługi ochrony dostępu przetwarzają w sposób zautomatyzowany wiele sygnałów logowania, np. lokalizację, czas, jaki upłynął od ostatniego logowania, liczbę błędnie wprowadzonych poświadczeń i wiele bardziej złożonych parametrów. Może to pomóc w wykryciu i określeniu poziomu ryzyka dla każdej próby uzyskania dostępu. Jeśli wystąpi nietypowa korelacja, usługa może zastosować ocenę ryzyka. Użytkownik wysokiego ryzyka powinien zostać zablokowany przed dostępem do systemu. Można to zrealizować za pośrednictwem zasad dostępu warunkowego dla dowolnej aplikacji zarejestrowanej w Azure AD. Administrator będzie musiał zweryfikować ryzyko, zanim użytkownik zostanie odblokowany. Z kolei użytkownik otrzyma komunikat o błędzie z instrukcją skontaktowania się z administratorem w celu ponownego włączenia dostępu.

Dostęp warunkowy to obecnie jeden z najlepszych sposobów na realizację wdrożenia zgodnego z koncepcją ograniczonego zaufania (Zero Trust).

Poufność

Pewne dokumenty i wiadomości przeznaczone są wyłącznie dla wybranych grup pracowników i zależy nam na tym, aby nie mogły zostać przeczytane lub edytowane przez użytkowników spoza tej grupy.

Taką funkcję realizują Etykiety Poufności. Zastosowane dla dokumentów i wiadomości zablokują otwarcie, odczyt czy edycję niepowołanym użytkownikom. Zaleca się, aby w ten sposób oznaczać wewnętrzne dokumenty zawierające dane osobowe lub dane wrażliwe. Współpraca na dokumentach zabezpieczonych Etykietą Poufności dla grupy upoważnionej przebiega identycznie jak w przypadku niezabezpieczonych treści i nie wiąże się z ograniczeniami.

Dzięki narzędziom raportowym uczelnia uzyskuje wiedzę na temat klasyfikacji informacji, która była stosowana wewnątrz organizacji. Każdy typ etykiety i czynności związane z oznakowanym dokumentem są logowane w czasie rzeczywistym

i przechowywane standardowo przez 30 dni. Etykiety mogą być stosowane automatycznie, np. w oparciu o wyrażenia algorytmiczne (np. wykrywające numer PESEL) lub własne wyrażenia i frazy. Na przykład oznakowanie dokumentu przechowywanego w chmurze sygnaturą BIO-10 skutkować będzie automatycznym nałożeniem odpowiedniej ochrony przez nadanie Etykiety Poufności. Etykiety stosowane dla poczty pozwalają ograniczyć jej dalsze przesyłanie. Również dla adresatów spoza organizacji. Uczelnia może stosować nietrwałe wiadomości e-mail, tzn. takie, których nie można otworzyć po upływie określonego czasu skonfigurowanego w zasadach dla tej etykiety. Ich stosowanie może być zautomatyzowane. Wiadomości spełniające określone kryteria otrzymają stosowne etykiety klasyfikacji i ochrony informacji od razu po wysłaniu, bez udziału użytkownika.

Udostępnianie

Przetwarzanie w chmurze otwiera nowe możliwości pracy i współpracy. Uczelnia powinna mieć jednak zarządczy wgląd do czynności podejmowanych przez użytkowników w chmurowych zasobach. Nie chodzi wyłącznie o dzienniki logowań. Czasami musimy wiedzieć, kto, kiedy i na jakim urządzeniu zmodyfikował, usunął czy przesunął istotny dokument. Uczelnia może zabronić drukowania, pobierania lub kopiowania treści dokumentów w przeglądarce na urządzeniach prywatnych (technologią, nie procedurą). Dzienniki standardowo dostępne w usługach chmurowych pozwalają na wgląd do wielu aktywności użytkowników, jednak bardziej praktyczne zastosowanie mają narzędzia pośredniczące i zapisujące czynności zachodzących w chmurze uczelni. Taką rolę pełni np. Microsoft Defender for Cloud Apps.

Wykrycie określonego typu działania generuje alert oraz odpowiednią czynność zarządczą. Jeśli w ciągu godziny użytkownik zaloguje się skutecznie z Polski, a następnie z Francji, to być może należy automatycznie zablokować mu dostęp. Scenariusz niemożliwej do zrealizowania podróży użytkownika powinien wyzwolić akcję odpowiednią do poziomu ryzyka.

Inny praktyczny scenariusz wykorzystania: uczelnia zazwyczaj nie kontroluje udostępniania plików na zewnątrz. Standardowo każde udostępnienie anonimowe z OneDrive jest bezterminowe i może być wykorzystane wielokrotnie przez wszystkie osoby posiadające link. Prawdopodobnie słusznym działaniem w tej sytuacji jest automatyczna anulacja dostępu po określonym czasie, który upłynął od przekazania linku lub ostatniej modyfikacji dokumentu. Nadmierne udostępnianie może być powodem wycieku istotnych danych.

ZARZĄDZANIE URZĄDZENIAMI

Ograniczenia

Urządzenia, podobnie jak użytkownicy, posiadają swoją tożsamość. Na tej podstawie można kontrolować dostęp do zasobów uczelni. Podział na urządzenia zarządzane i niezarządzane ma kluczowe znaczenie dla ochrony danych.

Bez objęcia zarządzaniem urządzeń należących do uczelni egzekwowanie zasad zabezpieczeń na podstawie technologii jest bardzo utrudnione – o ile nie całkowicie niemożliwe.

Czy komputer lub telefon służbowy są automatycznie lepiej zabezpieczone? Niekoniecznie. Sama możliwość wykonania pewnych czynności, np. pobrania danych na komputer służbowy, podczas gdy na prywatnym komputerze pobieranie jest zablokowane, jeszcze nie oznacza, że dane i sam użytkownik są bezpieczniejsze. Ochrona przed wyciekiem wymaga konfiguracji. W przeciwnym wypadku użytkownik bez praw administracyjnych i tak zainstaluje niezatwierdzoną przeglądarkę, zaloguje się do prywatnego zasobu w chmurze i skopiuje tam dane, do których ma uprawniony dostęp.

Zarządzanie jest jedynym sposobem na zautomatyzowaną ochronę zwłaszcza w organizacjach o dużej skali – a takimi są uczelnie.

Szyfrowanie

Brak szyfrowania danych spoczynkowych – czyli wtedy, gdy nie działa system Windows – był dla wielu uczelni powodem do zmartwień. Dysk takiego urządzenia może zostać użyty w innym komputerze, a to pozwala na uzyskanie nieautoryzowanego dostępu do danych poufnych i osobowych.

Aby się przed tym chronić, należy stosować szyfrowanie dla Windows Pro / Enterprise technologią BitLocker. Problem w tym, jak egzekwować procedurę szyfrowania na każdym urządzeniu i u każdego użytkownika. Przepisy nie pomogą. Wymagane jest zarządzanie urządzeniami. Dzięki temu możemy metodycznie stosować jednakowe zasady dla wszystkich urządzeń oraz, co równie ważne, udowodnić, że faktycznie je stosowaliśmy. Zwłaszcza w sytuacji losowej, gdy urządzenie zostanie skradzione.

Szyfrowanie dysków na komputerach Windows 10/11 (z TPM 2.0) zarządzanych i podłączonych do Azure AD nie wymaga interakcji użytkownika. Dzieje się w tle oraz nie wpływa negatywnie na wydajność współczesnych komputerów. Szyfrowanie powinno dotyczyć także nośników zewnętrznych. Uczelnia może wprowadzić politykę automatycznego szyfrowania dysków USB. Na nośnikach zewnętrznych pozbawionych ochrony BitLocker użytkownik nie będzie mógł zapisać plików pochodzących z komputera służbowego.

Utrata urządzenia lub nośnika zawierającego istotne informacje lub dane osobowe nie spowoduje ich wycieku, ponieważ zastosowano adekwatne ograniczenia techniczne blokujące korzystanie z danych uczelni przez osoby nieuprawnione.

Aktualizacje

Korzystanie z aktualnego i wspieranego przez producenta oprogramowania to podstawowa i najstarsza z zasad

cyberbezpieczeństwa. Tego typu rekomendacje znajdziemy w publikacjach większości instytucji zajmujących się zaleceniami w tym obszarze.

Wynika z tego, że uczelnie, które chcą zachować zgodność z rekomendacjami, powinny dysponować mechanizmem kontrolowanej aktualizacji dla systemu operacyjnego i wykorzystywanych aplikacji. Taką kontrolę i ewidencję stosowanych zasad, czyli zarządzanie aktualizacjami, znajdziemy np. w Intune oraz Microsoft Defender for Endpoint. Tylko zarządzane urządzenia pozwalają na kontrolę nad aktualizacjami i dotrzymanie terminów, zwłaszcza w skali tak dużej, jak uczelnia.

Mobilność

Większość użytkowników korzysta z telefonów komórkowych, a usługi w chmurze standardowo pozwalają na dostęp z dedykowanych aplikacji mobilnych (np. poczta elektroniczna, Teams, Word, SharePoint, Planner itd.). Oznacza to, że dane uczelni mogą być przetwarzane na telefonach – prywatnych albo służbowych, jednak najczęściej niezarządzanych. Czy istnieje między nimi różnica w dostępie? Żadna. Niezarządzany telefon to prywatny telefon. Generuje to ryzyko związane z brakiem wpływu właściciela danych (uczelnia) na bezpieczeństwo ich przetwarzania (telefon użytkownika).

Jeśli wdrożenie zarządzania platformą mobilną wykracza poza organizacyjne możliwości uczelni, zaleca się stosowanie technologii ochrony informacji należących do uczelni w aplikacjach mobilnych. Dzięki temu zamiast zarządzać całym urządzeniem, chronimy tylko informacje uczelni (czyli takie pozyskane przez login uczelniany) w ogólnodostępnych aplikacjach mobilnych Microsoft. Takie informacje nie będą mogły zostać przekazane do prywatnych zasobów w chmurze (również z postaci kopii zapasowej), nie będą mogły zostać skopiowane do prywatnych aplikacji (funkcja kopiuj-wklej nie będzie działać), a dostęp będzie chroniony przynajmniej PINem, ponieważ ostatecznie nie wiemy, czy użytkownik korzysta z jakiegokolwiek zabezpieczenia swojego telefonu.

Pamiętajmy, aby jednocześnie zablokować dostęp do zasobów uczelni z mobilnej przeglądarki. W przeciwnym wypadku ochrona w aplikacji nie zabezpieczy uczelni skutecznie.

ZARZĄDZANIE RYZYKIEM

Wyciek

Wyciek kojarzy się nam z zewnętrznym i złośliwym działaniem. Jednak wyciek może być wynikiem umyślnego działania użytkownika wewnętrznego. Skoro nawet na urządzeniu służbowym, oczywiście po kompletnym i skutecznym uwierzytelnieniu, możemy zalogować się do prywatnej poczty, a następnie dodać do prywatnej wiadomości załącznik, który jest poufnym dokumentem stanowiącym np. własność intelektualną uczelni, to właśnie mamy do czynienia z wyciekiem informacji. W tym konkretnym scenariuszu żadna procedura nie będzie stanowić skutecznej ochrony. Można jednak zastosować technologię. Automatyczne szyfrowanie dokumentów pochodzących z zasobów chmurowych uczelni lub jej zasobów dyskowych pozwala zablokować przekazywanie dokumentów, zdjęć, filmów przez przeglądarkę do prywatnych zasobów w chmurze (np. osobisty OneDrive, G-Drive czy Dropbox). Uczelnia nie musi blokować korzystania z nośników USB, aby zabezpieczyć swoją własność. Pliki zostaną skopiowane w wersji zaszyfrowanej i nie pozwolą się otworzyć, gdy użytkownik straci tożsamość w systemie uczelni (straci konto).

Inny przykład wycieku jest niemożliwy do zablokowania bez technologii zabezpieczeń lub na urządzeniach niepodłączonych do domeny. Każdy użytkownik z licencją na OneDrive może na dowolnym komputerze zainstalować darmową aplikację OneDrive.exe i po skutecznym zalogowaniu dokonać synchronizacji wszystkich swoich danych przechowywanych na OneDrive. Od tego momentu uczelnia nie ma wpływu na

dalszy cykl życia tych informacji. Dodatkowo synchronizator OneDrive to jedyna aplikacja do pobierania zawartości witryn SharePoint oraz plików zespołu Teams. Standardowe ustawienia obu aplikacji pozwalają na synchronizację danych z chmury do urządzenia użytkownika. Należy to ryzyko zaakceptować albo zaadresować przez Dostęp Warunkowy, blokując użycie OneDrive.exe na urządzeniach niezarządzanych lub zablokować całkowicie dla użytkowników wysokiego ryzyka. Będzie to miało wpływ również na instalowaną na komputerze aplikację Teams.

Administrator

Często ostatecznym celem ataku jest administrator, czyli użytkownik uprzywilejowany. Skorzystanie z jego uprawnień daje nieograniczone możliwości do nadużyć. Liczba użytkowników z permanentnie aktywnymi, najwyższymi uprawnieniami powinna być ograniczona do niezbędnego minimum. Microsoft rekomenduje nie więcej niż 5 – ale więcej niż 1 administratora z najwyższym zakresem uprawnień. Do realizacji zadań administracyjnych należy korzystać z najniższych możliwych uprawnień umożliwiających realizację czynności. W praktyce oznacza to, że nie każde zadanie wymaga roli administratora globalnego.

W usługach chmurowych Microsoft (Teams, Exchange, Microsoft Endpoint Manager itd.) istnieją adekwatne role administracyjne przeznaczone do zarządzania każdym obszarem. Modelem zalecanym jest jednak działanie *just in time*, czyli czasowe uruchomienie uprawnień administracyjnych wyłącznie na potrzeby realizacji działań konfiguracji usług i nie dłużej niż przez 8 godzin. Wyższe plany usług Microsoft oferują takie mechanizmy. Dzięki temu każda uczelnia może dysponować procesem zarządzanym technologicznie, gwarantującym najniższe możliwe uprawnienia udzielane na życzenie i automatycznie anulowane po upływie określonego czasu. Przydzielanie i aktywowanie uprawnień jest w pełni monitorowane. Aktywacja wysoce uprzywilejowanych ról wymaga zatwierdzenia – w uzasadnionych przypadkach nawet więcej niż jednego administratora. Uprawnienia nie są trwałe. Narzędzie pozwala również na łatwiejsze przeprowadzenie cyklicznego przeglądu uprawnień, który powinien być rutyną każdej organizacji.

Uczelnie często korzystają z synchronizacji pomiędzy lokalnym Active Directory a Azure Active Directory. W tym przypadku wysoce uprzywilejowane konta użytkowników powinny być dostępne wyłącznie w chmurze (bez synchronizacji).

Do uwierzytelniania administracyjnego powinno być wymagane urządzenie zarządzane i kontrolowane przez uczelnię.

Awaria

Systemy uwierzytelnienia wieloskładnikowego zależą od dodatkowego składnika zatwierdzania logowania, w praktyce najczęściej telefonu komórkowego. W sytuacji awaryjnej – gdy sieć komórkowa nie działa lub gdy utracimy aplikację – logowanie do systemu nie będzie możliwe. Dotyczy to również administratorów. Dlatego należy skonfigurować konta dostępu awaryjnego, które wyłączone są ze standardowych zasad logowania wieloskładnikowego. Konta takie nie mogą być zależne od tych

samych czynników i infrastruktury logowania (np. sieć komórkowa), od których zależy dostęp regularnych administratorów.

Konto typu *Break Glass* jest konieczne. Jednak gdy nie jest objęte uwierzytelnieniem wieloskładnikowym, może stanowić jeszcze większy element ryzyka niż brak takiego konta. Zaleca się, aby konta awaryjne korzystały z innej metody uwierzytelnienia niż regularny administrator globalny - z metody odpornej na awarię jednego systemu autoryzacji. Takim rozwiązaniem może być skonfigurowanie dostępu opartego na kluczach FIDO2 służących do logowania się bez użycia hasła.

ZARZĄDZANIE ZAGROŻENIAMI

Ransomware

Ataki wirusów szyfrujących (ransomware, oprogramowanie dla okupu) jest poważnym zagrożeniem, które paraliżuje działanie całych organizacji na długi czas. Ryzyko wystąpienia ataku jest wysokie. Złośliwy kod zostaje przekazany najczęściej przez fałszywy załącznik w wiadomości e-mail. Może zostać zatrzymany przez oprogramowanie antywirusowe. Warunek jest jeden – kod musiał być znany i wprowadzony do sygnatur ochrony antywirusowej. Większość oprogramowania antywirusowego nie zareaguje na nieznane dotychczas wirusy przez wykrywanie anomalii w działaniu systemu. Aby ograniczać ryzyko ransomware, należy korzystać z bardziej zaawansowanych narzędzi, które reagują na anomalie zachodzące w procesach systemu operacyjnego. Usługą zalecaną jest Microsoft Defender for Endpoint.

Jednak można się chronić również dzięki odpowiedniej konfiguracji. OneDrive for Business przechowuje nie tylko bieżącą wersję pliku Office, ale również poprzednie. W przypadku szyfrowania poprzednie wersje nie zostaną zablokowane i będzie można je odzyskać. Funkcja kontrolowanego dostępu do folderów użytkownika nie pozwoli natomiast na ingerencję w foldery przez niezaufane procesy. Pliki nie będą mogły zostać zablokowane. Ochrona obszaru ataku (ASR, Attack Surface Reduction) to zbiór reguł i blokad, które pomagają zapobiegać podejrzanemu zachowaniu oprogramowania. To wzorce działania wykorzystywane zazwyczaj przez złośliwe oprogramowanie, stosowane w celu przełamania zabezpieczeń urządzenia. Do skutecznego wdrożenia potrzebne jest zarządzanie urządzeniami.

Incydenty

Chmura ciągle się zmienia. Zmieniają się również obszary zagrożeń i metody ataku. Każda instytucja przetwarzająca istotne dane powinna być na bieżąco – zarówno z możliwościami usług w chmurze, jak i zmieniającymi się rekomendacjami. Potrzebna jest stała informacja o stanie zabezpieczeń i odporności infrastruktury uczelni na wykryte podatności. Uczelnia powinna monitorować wdrożone produkty bezpieczeństwa, kontrolować stan usług, analizować występujące ataki i wiedzieć, jak się przed nimi bronić.

Wiele różnych produktów zabezpieczających z rodziny Microsoft Defender generuje alerty, incydenty i wykrycia. Jeśli uczelnia nie reaguje na incydenty i nie zarządza nimi, może znaleźć się w trudnej sytuacji reagowania na skuteczny atak lub wyciek.

Zarządzanie incydentami i klasyfikacja zagrożeń mogą być początkowo trudne, jednak automatyzacja w agregacji alertów pomaga ograniczać ilość informacji, które należy analizować. Usługa Azure Sentinel pozwala na łatwe agregowanie alertów i logów w jednym miejscu. Obsługuje zarówno dane lokalne, jak i dane w chmurze.

Ponieważ wiele własnych łączników danych dla Azure Sentinel jest bezpłatnych, koszt wykorzystania usługi może być minimalny, a istotnie podnosi poziom monitoringu incydentów dotyczących naruszenia zabezpieczeń.

4 Wnioski

W czasie wdrożenia dodatkowych rozwiązań technologicznych, wymuszonego dostosowaniem życia uczelni do warunków pandemicznych, jego tempo mogło wpłynąć niekorzystnie na poziom stosowanych zabezpieczeń.

Do skutecznej ochrony potrzebne są zarówno procedury, jak i technologia. Skala działania uczelni nie pozostawia wątpliwości, że sygnałów mogących wskazywać na naruszenie zabezpieczeń nie da się przeanalizować manualnie. Bez technologii procedury pozostaną wyłącznie intencją zabezpieczenia.

Należy pamiętać, że podstawowe narzędzia do pracy i współpracy nie zawierają technologii zabezpieczeń. Nie można liczyć na zaawansowaną ochronę, korzystając z podstawowych wersji i subskrypcji. Jeśli cyberbezpieczeństwo nie stanie się elementem budżetu uczelni, trudno będzie mówić o poziomie ochrony stosownym do ponoszonego ryzyka. Uczelnie mogą zapłacić za bezpieczeństwo lub za jego brak.

Odpowiedzialny proces cyfryzacji nauki i szkolnictwa wyższego powinien obejmować:

1. Dokonanie ewaluacji wykorzystywanej aktualnie infrastruktury informatycznej oraz systemu oprogramowania z udziałem ekspertów branży technologicznej.
2. Dostosowanie planu licencyjnego lub rozwiązań technologicznych, tak aby właściwie zabezpieczyć komunikację, tożsamość, dostęp, urządzenia, kontrolować ryzyko i zagrożenia podczas korzystania społeczności uczelni z narzędzi cyfrowych.
3. Edukację społeczności akademickiej o tym, jak bezpiecznie korzystać z narzędzi cyfrowych i jak odpowiedzialnie zachowywać się w sieci.

5 Oferta Microsoft dla bezpiecznej uczelni

Aby dowiedzieć się więcej o możliwościach współpracy z firmą Microsoft i jej Partnerami w obszarze cyberbezpieczeństwa, zapraszamy do kontaktu ze swoim opiekunem lub przedstawicielami Partnerów Microsoft. Jeśli zastanawiają się Państwo, kto jest opiekunem Państwa uczelni, prosimy o kontakt na adres mailowy edukacja@microsoft.com.

Plany licencyjne

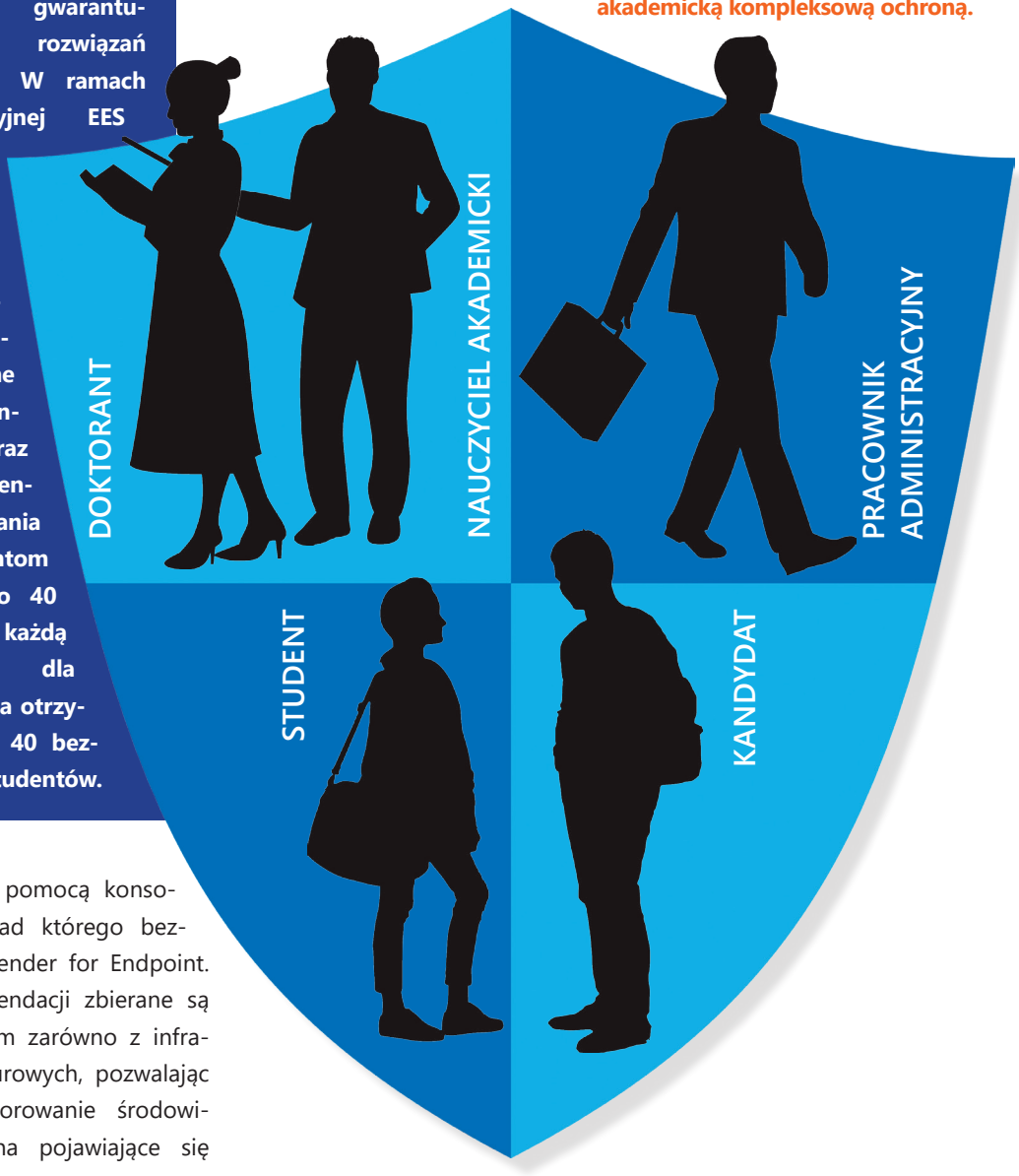
Zakup planów Microsoft 365 A3 lub A5 gwarantuje standaryzację rozwiązań w całej organizacji. W ramach umowy subskrypcyjnej EES uczelnie, kupując licencję dla wszystkich pracowników naukowo-dydaktycznych i administracyjnych, otrzymują ujednolicone, bezpieczne środowisko do codziennej pracy i nauki wraz z bezpłatnymi licencjami do udostępniania wszystkim studentom w przeliczeniu 1 do 40 – co oznacza, że za każdą zakupioną licencję dla wykładowców uczelnia otrzymuje prawo do aż 40 bezpłatnych licencji dla studentów.

Plany Microsoft 365 A3 oraz Microsoft 365 A5 uwzględniają potrzeby użytkowników zarówno pod kątem dostępu do ujednoliconej, najnowszej wersji aplikacji pakietu Office, systemu operacyjnego Windows 10 i 11 Pro, jak również zabezpieczeń poczty, tożsamości użytkowników i zabezpieczeń dostępu do przechowywanych i udostępnianych plików pracowników oraz studentów.

Niezależnie od liczby komputerów w organizacji standaryzacja oprogramowania Office i Windows 10 i 11 Pro obejmuje wszystkie stacje robocze na uczelni, tworząc

Zakup planów Microsoft 365 A3 lub A5 gwarantuje standaryzację rozwiązań w całej organizacji. W ramach umowy subskrypcyjnej EES uczelnie kupując licencję dla wszystkich pracowników naukowo-dydaktycznych i administracyjnych otrzymują ujednolicone, bezpieczne środowisko do codziennej pracy i nauki wraz z bezpłatnymi licencjami do udostępniania wszystkim studentom w przeliczeniu 1 do 40 – co oznacza, że za każdą zakupioną licencję dla wykładowców uczelnia otrzymuje prawo do aż 40 bezpłatnych licencji dla studentów.

Rozwiązania planów A3 i A5 obejmują społeczność akademicką kompleksową ochroną.



w pełni zarządzane środowisko za pomocą konsoli Microsoft Endpoint Manager, nad którego bezpieczeństwem czuwa Microsoft Defender for Endpoint. Dane dotyczące zagrożeń i rekomendacji zbierane są w jednym centrum administracyjnym zarówno z infrastruktury lokalnej, jak i usług chmurowych, pozwalając administratorowi na pełne monitorowanie środowiska i błyskawiczne reagowanie na pojawiające się podejrzane zdarzenia.

Najnowsza technologia to jednak nie wszystko. Niezwykle istotna jest edukacja użytkowników i wypracowanie właściwych reakcji na potencjalne próby ataków i przyzwyczajeń w codziennej pracy. Aby wyzwolić czujność użytkowników i pozwolić im uczyć się na błędach, w planie Microsoft 365 A5 dostępne są symulatory ataków, przypominające wiadomości mające na celu wykradnięcie danych organizacji, dostępu do konta czy pobranie niechcianego oprogramowania. Symulacja ataków pozwoli administratorowi na ocenę świadomości użytkowników w zakresie cyberbezpieczeństwa, a pracownikom na oswojenie się z technikami stosowanymi przez hakerów w kontrolowanych warunkach.

Plan Microsoft 365 A5 pozwala jednak na znacznie więcej. Daje on również możliwość zastąpienia klasycznej telefonii na uczelni telefonią w aplikacjach Teams. Ograniczenie liczby rozwiązań i unifikacja usług dostępnych na uczelni pozwoli na dogłębne poznanie jednej technologii, przyzwyczajenie użytkowników do jednego loginu i hasła oraz prostsze zarządzanie zintegrowanymi usługami przez administratorów.

Najwyższy poziom bezpieczeństwa gwarantuje objęcie wszystkich pracowników licencjami Microsoft 365 A5, jednak często spotykanym scenariuszem jest zakup licencji w planie A5 dla wybranej grupy, np. władze uczelni, pracownicy dziekanatu i obsługi studentów, którzy mają na co dzień do czynienia z danymi wrażliwymi, danymi osobowymi lub mają wyższe uprawnienia w organizacji włącznie z uprawnieniami administracyjnymi.

Zasadnicze różnice pomiędzy Microsoft 365 A3 a A5 dotyczą 4 obszarów:

BEZPIECZEŃSTWA

Dzięki zintegrowanym i zautomatyzowanym zabezpieczeniom rozszerza ochronę tożsamości przed zagrożeniami oraz szkodliwymi atakami

ZGODNOŚCI

Łączą w sobie ochronę informacji oraz zaawansowane możliwości zapewnienia zgodności w celu ochrony danych i zarządzania nimi przy jednoczesnym zmniejszeniu ryzyka

ANALITYKI

Usługi PowerBI, które pomagają uzyskać znaczącą wartość biznesową z dostępnych źródeł danych, ułatwiając analitykę i wizualizację danych

TELEFONII VOIP

Funkcje konferencji audio i połączeń telefonicznych w chmurze

6 Rekomendacje

JAK KORZYSTAĆ Z ROZWIĄZAŃ MICROSOFT, ABY SKUTECZNIE ZADBAĆ O CYBERBEZPIECZEŃSTWO NA UCZELNI

Ochrona tożsamości i ochrona dostępu

1. Stosujmy uwierzytelnianie wieloskładnikowe do wszystkich usług w chmurze; konfigurowane przez zasady, nie manualnie per użytkownik (Multi-Factor Authentication, Conditional Access).
2. Wykorzystujmy klucze sprzętowe FIDO2 zamiast haseł (Passwordless, FIDO2).
3. Stosujmy zasady dostępu warunkowego, spójne i dostosowane dla grup docelowych (Conditional Access).
4. Zalecamy wyłączenie protokołów poczty starszego typu IMAP/POP/SMTP (Exchange Online).
5. Ograniczajmy ilość loginów, na korzyść jednego systemu uwierzytelniania (Azure AD).
6. Uprawnienia administracyjne powinny być udzielane na określony czas i dopasowane do czynności, które należy wykonać, zgodnie z zasadą najniższych możliwych uprawnień (Azure AD Privileged Identity Management).
7. Zabezpieczajmy dostęp administracyjny przez stosowanie kont dostępu awaryjnego (Break Glass Account, Conditional Access).

Ochrona przed zagrożeniami

1. Korzystajmy z technologii zaawansowanej weryfikacji załączników poczty; filtracja załączników w oparciu o typ pliku nie jest wystarczająca (Safe Attachments).
2. Należy stosować zasady ochrony dla zredukowania obszarów potencjalnych ataków (Attack Surface Reduction).
3. Korzystajmy z zarządzanego systemu antywirusowego oraz z usług inteligentnych analizujących i reagujących na anomalie wykryte w procesach systemu operacyjnego (Microsoft Defender for Endpoint).

Zarządzanie urządzeniami

1. Należy zarządzać urządzeniami w sposób scentralizowany (Microsoft Intune).
2. Ograniczajmy możliwości korzystania z danych uczelni na urządzeniach niezarządzanych (Microsoft Intune, Microsoft Defender for Cloud Apps).
3. Należy zarządzać urządzeniami mobilnymi, dostępem mobilnym do usług i chronić informacje uczelni przetwarzane na telefonach i w przeglądarkach (Microsoft Intune, App Protection Policies).

Ochrona informacji

1. Ochrona dostępu nie chroni przed wyciekiem, szyfrujmy dane wewnętrzne uczelni, aby stały się bezużyteczne po zablokowaniu konta użytkownika (DLP for Endpoint, Windows Information Protection).
2. Poufność dokumentów i wiadomości należy chronić na podstawie technologii, zalecane jest szyfrowanie przy użyciu Microsoft Purview Information Protection, również w pełni zautomatyzowane (Sensitivity Labels, Microsoft Defender for Cloud Apps).
3. Dyski komputerów muszą być zaszyfrowane technologią BitLocker (Windows Enterprise, Microsoft Endpoint Manager).

Monitoring

1. Cyklicznie weryfikujmy konfigurację poczty, reguły serwera poczty oraz stosowane wyjątki (środki organizacyjne oraz techniczne np. Exchange Configuration Analyzer).
2. Należy monitorować czynności, jakie użytkownicy podejmują w aplikacjach chmurowych oraz korzystać z alertów wyzwalanych przez niepożądane lub podejrzane działania (Microsoft Defender for Cloud Apps).
3. Kontrolujmy nadmierne udostępnianie (Microsoft Defender for Cloud Apps).
4. Monitorowanie incydentów bezpieczeństwa pozwala uchronić się przed skutkami włamania (Azure Sentinel).

JAK ZADBAĆ O CYBERBEZPIECZEŃSTWO JUŻ TERAZ

1. Dbajmy o mocne hasło i wieloskładnikowe uwierzytelnianie podczas logowania.
2. Warto stosować klucz zabezpieczeń, metody bez użycia hasła.
3. Zastosujmy zasadę ograniczonego zaufania i nadajmy uprawnienia w najmniejszym niezbędnym do pracy zakresie.
4. Należy pamiętać o szyfrowaniu dokumentów i zabezpieczeniu dostępu hasłami.
5. Korzystanie z aktualnego oprogramowania producenta i nieodkładanie instalacji poprawek bezpieczeństwa na później to również istotna kwestia do zapamiętania.
6. Kontrolujmy pliki udostępniane na zewnątrz organizacji.

Zawsze edukujmy użytkowników i podwyższajmy świadomość społeczności akademickiej w obszarze bezpieczeństwa w cyberprzestrzeni!

Uczelnia w Chmurze Microsoft to:

: Uczelnia na wyznaczonej przez Microsoft Education Transformation Framework ścieżce cyfrowej transformacji, dążąca do ciągłego usprawniania pracy poprzeć wdrażanie najnowocześniejszych narzędzi i optymalne wykorzystanie danych.

: Uczelnia bezpieczna, która chroni studentów i obiekty za sprawą kompleksowego asortymentu zintegrowanych rozwiązań edukacyjnych i inteligentnych zabezpieczeń dla szkolnictwa wyższego.

: Uczelnia, która rozumie i inwestuje w bezpieczną i wydajną infrastrukturę informatyczną, wspierającą pracę uczelni we wszystkich jej wymiarach. Uczelnia dająca studentom nie tylko wykształcenie, ale też praktyczne umiejętności. Oprogramowanie, inicjatywy i technologie Microsoft dla szkolnictwa wyższego pomagają przygotować studentów na przyszłość. Przekazują im kompetencje, które czynią ich gotowymi na realne wyzwania, jakie niesie przyszłość.

: Uczelnia, która przyciąga najlepszych. Tworzy warunki, w których będą oni osiągać optymalne wyniki, i doskonali swoją działalność przy użyciu rozwiązań Microsoft dla szkolnictwa wyższego.

: Uczelnia, która nieustannie się rozwija i prowadzi badania naukowe w chmurze Microsoft Azure. Dzięki tej otwartej, elastycznej i globalnej platformie, obsługującej różne języki programowania, narzędzia i struktury, pracownicy naukowi mogą skrócić czas badań i zoptymalizować ich koszty.

Microsoft

Na całym świecie Microsoft pomaga szkołom i uczelniom realizować w pełni ich potencjał

aka.ms/uczelniawchmurze