AUDYT BEZPIECZEŃSTWA

Niniejszy dokument przedstawia zanonimizowane wyniki audytu bezpieczeństwa, przeprowadzonego z wykorzystaniem rozwiązania Safetica. Audyt zrealizowano na 83 stacjach roboczych w okresie od 1 marca do 19 marca 2019 roku. Dane odnoszą się do godzin pracy audytowanego przedsiębiorstwa (7:00–16:00).

safetica®

Zawartość

ZAKRES AUDYTU

Audyt bezpieczeństwa koncentruje się na wrażliwych plikach w środowisku firmy, plikach opuszczających firmę oraz na tym, w jaki sposób pracownicy wykorzystują zasoby firmowe.

Audyt jest oparty na monitorowaniu plików i aktywności użytkowników komputerów, na których wdrożono rozwiązanie Safetica. Bezpieczeństwo i zalecane środki ostrożności są oceniane na podstawie tego, które pliki w Safetica zostały sklasyfikowane jako wrażliwe, jakie bezpieczne metody wybrane zostały do przesyłania poufnych treści i jakie akcje użytkowników zostały zaklasyfikowane jako ryzykowne.

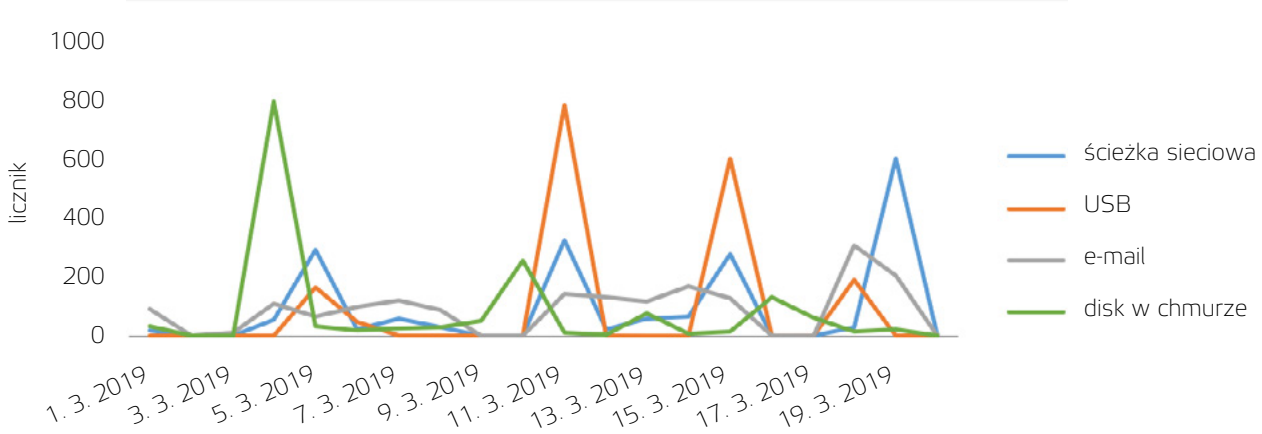
Monitorowane dane:

- **301 GB** danych
- **91.599** operacje na plikach
- **33.032** pliki
- **4.240** pliki wychodzące

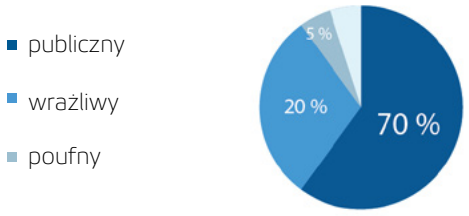
Monitorowane środowisko:

- **321** konta użytkowników
- **83** komputerów z zainstalowaną aplikacją Safetica
- **223** wszystkich komputerów
- **42** administratorzy Safetica

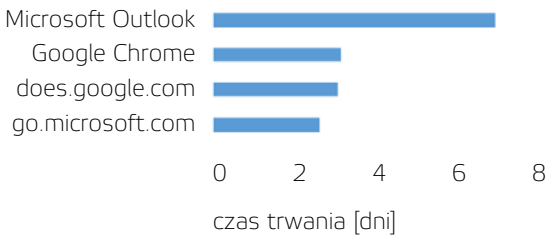
Kiedy wysłano pliki?



Do jakich kategorii należały wysyłane pliki?



Jakie były najczęstsze aktywności?



W przypadku incydentu bezpieczeństwa otrzymasz natychmiastowe powiadomienie.

Jeśli wystąpi zagrożenie bezpieczeństwa, szybka reakcja jest kluczowa, aby zminimalizować negatywne skutki. Natychmiastowe alerty przesyłane do odpowiednich osób pomogą szybko zlokalizować problem.

Skonfigurowałeś regularne raporty dotyczące bezpieczeństwa firmy.

Regularna kontrola stanu bezpieczeństwa firmy jest istotną częścią ogólnej strategii bezpieczeństwa.

Zidentyfikowałeś poufne dane firmowe, które muszą być chronione.

Nie wiedząc, jakie są wrażliwe dane firmy, nie można zastosować polityki bezpieczeństwa, aby zapobiec wyciekom.

Doporučení:

- Ustaw natychmiastowe powiadomienia dla wszystkich incydentów bezpieczeństwa, które chcesz monitorować.
- Sprawdź, czy natychmiastowe powiadomienia są aktualne i adresowane do właściwej osoby.
- Ustaw automatyczne raporty dotyczące odpowiednich obszarów.
- Sprawdź, czy raporty są aktualne i adresowane do właściwej osoby.
- Sprawdź, na jakich plikach pracują użytkownicy i zidentyfikuj wrażliwe dane.
- Regularnie klasyfikuj pliki zawierające wrażliwe dane.

PLIKI PRZENOSZONE NA NOŚNIKI USB I INNE URZĄDZENIA PRZENOŚNE

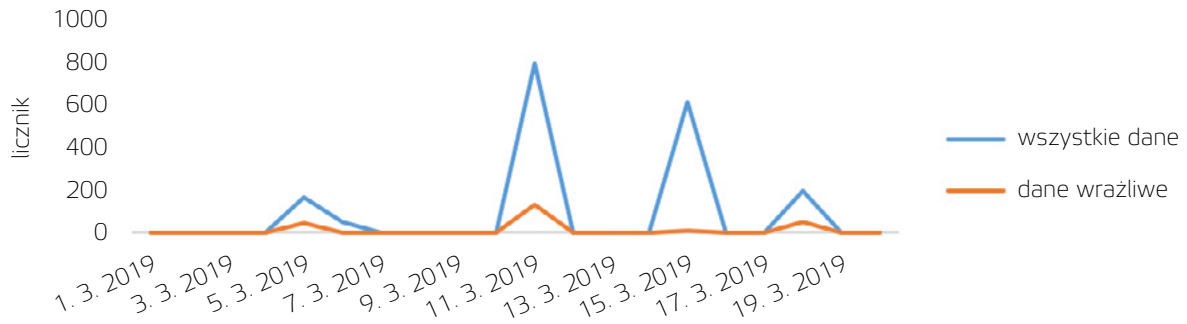
Kopiowanie dużej ilości wrażliwych plików na nośniki USB to szybki i łatwy sposób na utratę kontroli nad danymi. Jeśli nośnik USB zostanie zgubiony lub skradziony, krytyczne dane mogą wpaść w niepowołane ręce.

223 wrażliwych plików z 1793 plików zostało przesłanych przez nośnik USB lub inne urządzenie wymienne. Twoja polityka bezpieczeństwa nie była restrykcyjna.

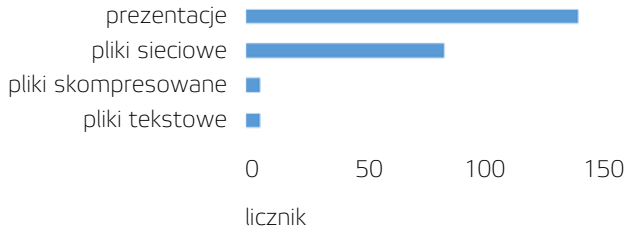
Przenoszenie danych firmowych przy wykorzystaniu nośników USB stanowi znaczne ryzyko. Zapewnienie bezpieczeństwa nośników USB jest niezbędne.

15 wrażliwych plików z 16 plików zostało przesłanych przez nośnik USB lub inne urządzenie wymienne. Te pliki były zgodne z polityką bezpieczeństwa.

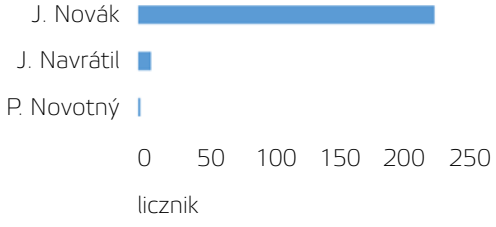
Kiedy wysłano pliki?



Jakie kategorie wrażliwych plików były przesyłane?



Kto przesłał najwięcej wrażliwych plików?



Zalecenia:

- Zdefiniuj i zweryfikuj, które nośniki USB są zaufane.
- Sprawdź jakie pliki są przenoszone. Zweryfikuj, czy któreś pliki nie powinny być sklasyfikowane jako wrażliwe.
- Ogranicz korzystanie z nośników USB i innych urządzeń wymiennych - tylko do odczytu lub zablokuj, jeśli urządzenie jest niezaufane.
- Ustaw reguły DLP dla wrażliwych plików przenoszonych na nośniki USB i inne urządzenia wymienne.
- Ustaw powiadomienie, kiedy wrażliwe pliki są przenoszone na niezaufanym urządzeniu wymiennym.
- Ustaw powiadomienia e-mail, kiedy pracownik kopiuje dużą ilość plików na nośnik wymienny.

PLIKI PRZESŁANE ZA POMOCĄ WIADOMOŚCI E-MAIL

Załączniki e-mail są jedną z najłatwiejszych metod przenoszenia danych i powodem wielu wycieków. W większości przypadków działanie nie jest celowe – przesłanie wiadomości na niewłaściwy adres lub dołączenie błędnego pliku.

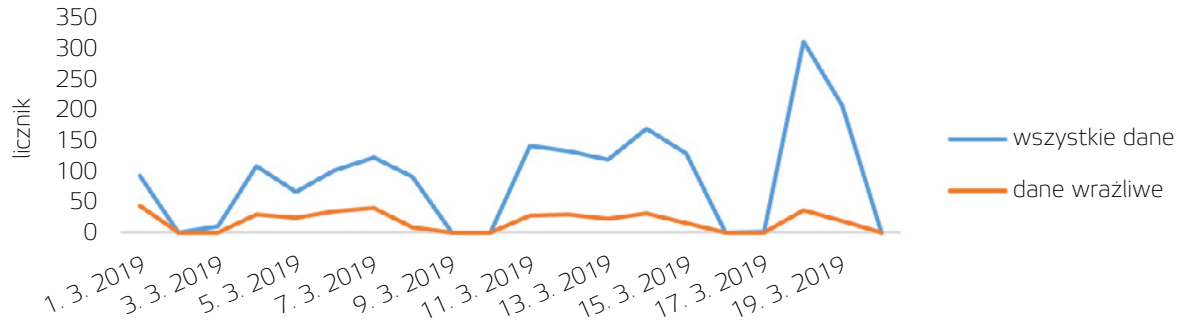
5 wrażliwych plików z 136 plików zostało przesłanych przez e-mail. Te pliki nie były kontrolowane przez jakąkolwiek politykę bezpieczeństwa.

Wiadomości e-mail z załączonymi wrażliwymi plikami powinny być wysyłane wyłącznie do zaufanych odbiorców, którzy mogą pracować na tego typu plikach.

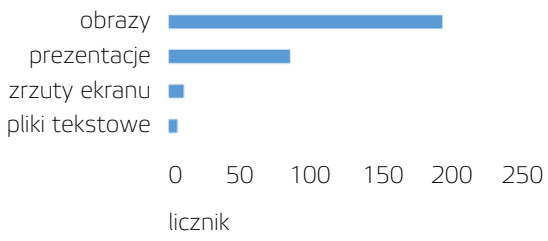
124 wrażliwych plików z 124 plików zostało przesłanych przez e-mail. Twoja polityka bezpieczeństwa nie była restrykcyjna.

241 wrażliwych plików z 1586 plików zostało przesłanych przez e-mail. Te pliki były zgodne z polityką bezpieczeństwa.

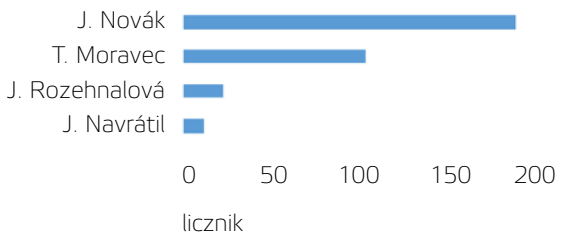
Kiedy wysłano pliki?



Jakie kategorie wrażliwych plików były przesyłane?



Kto przesłał najwięcej wrażliwych plików?



Zalecenia:

- Zdefiniuj i zweryfikuj zaufane domeny e-mail.
- Sprawdź jakie wiadomości są wysyłane z załącznikami. Oceń, czy załączone pliki nie powinny być zaklasyfikowane jako wrażliwe.
- Ustaw reguły DLP dla wrażliwych plików przesyłanych przez e-mail.
- Ustaw natychmiastowe powiadomienia, gdy wrażliwe pliki są przesyłane do niezaufanych domen e-mail.

PLIKI PRZESŁANE ZA POMOCĄ POCZTY WEBOWEJ

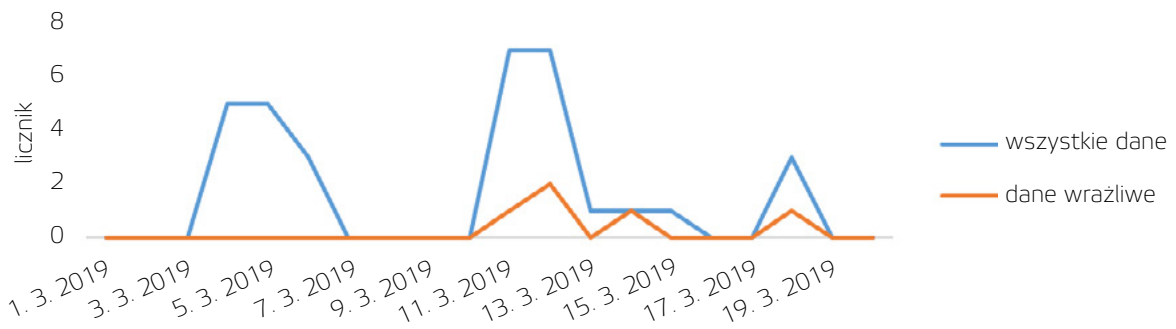
Poczta webowa jest często wykorzystywana do komunikacji i przesyłania poufnych plików. Jednocześnie taka forma komunikacji jest kolejnym kanałem ryzyka, który należy chronić przed potencjalnym wyciekiem.

3 wrażliwych plików z 31 plików zostało przesłanych przez poczta webowa. Twoja polityka bezpieczeństwa nie była restrykcyjna.

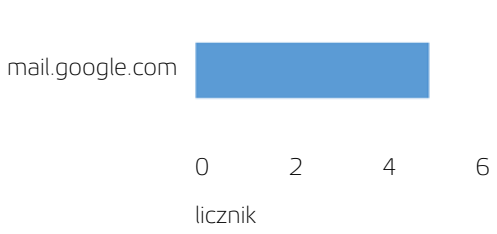
Korzystanie z usług poczty internetowej do przesyłania poufnych danych jest kwestią bezpieczeństwa, gdyż uniemożliwia kontrolę odbiorców danych.

2 wrażliwych plików z 2 plików zostało przesłanych przez poczta webowa. Te pliki były zgodne z polityką bezpieczeństwa.

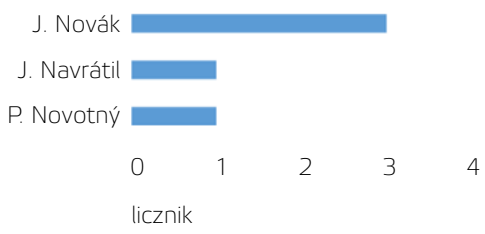
Kiedy wysłano pliki?



Gdzie przesyłano wrażliwe pliki?



Kto przesłał najwięcej wrażliwych plików?



Zalecenia:

- Zdefiniuj i zweryfikuj zaufane domeny e-mail.
- Sprawdź jakie pliki są przesyłane. Zweryfikuj, czy któreś pliki powinny być sklasyfikowane jako wrażliwe.
- Ustaw reguły DLP dla plików wrażliwych przesyłanych na pocztę webową.
- Ustaw powiadomienie, kiedy pliki wrażliwe są dołączane do wiadomości e-mail na pocztę webową.

FIRMOWE PLIKI PRZESŁANE DO INTERNETU

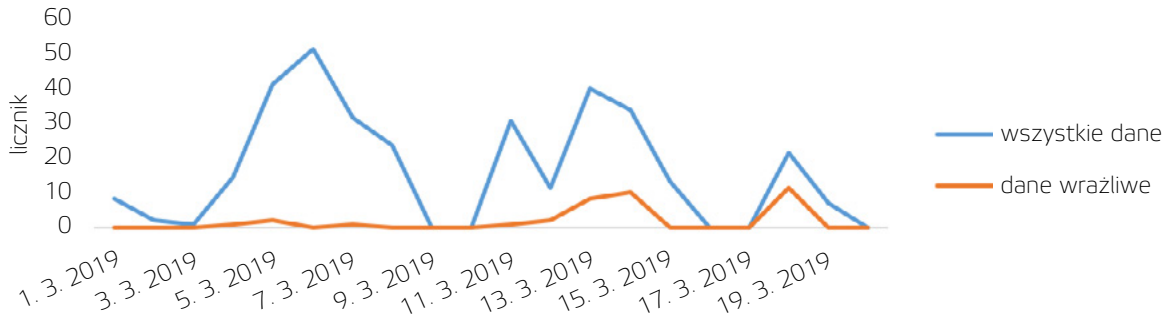
Przesyłanie plików do Internetu jest popularną metodą udostępniania pracownikom większych plików, których nie można wysłać w załączniku do wiadomości e-mail. Dlatego ważne jest określenie reguł korzystania z tego typu transferu.

11 wrażliwych plików z 301 plików zostało przesłanych przez przesyłanie na stronę internetową. Twoja polityka bezpieczeństwa nie była restrykcyjna.

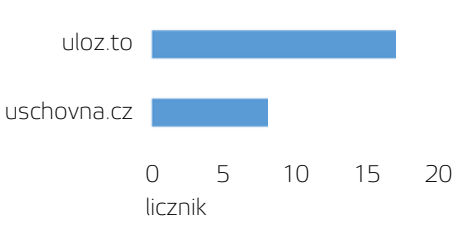
Pliki firmowe, które są przesyłane do publicznych witryn, mogą zostać pobrane przez nieznane osoby, co z kolei może prowadzić do utraty kontroli nad nimi.

25 wrażliwych plików z 25 plików zostało przesłanych przez przesyłanie na stronę internetową. Te pliki były zgodne z polityką bezpieczeństwa.

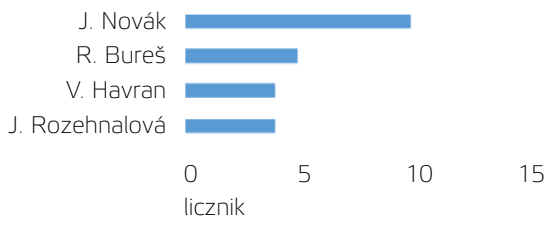
Kdy soubory odešly?



Gdzie przesyłano wrażliwe pliki?



Kto przesłał najwięcej wrażliwych plików?



Zalecenia:

- Zdefiniuj i zweryfikuj zaufane strony internetowe.
- Sprawdź jakie pliki są przesyłane. Zweryfikuj, czy któreś pliki powinny być sklasyfikowane jako wrażliwe.
- Ustaw reguły DLP dla wrażliwych plików przesyłanych na strony internetowe.
- Ustaw powiadomienie , kiedy wrażliwe pliki są przesyłane do niezaufanych stron internetowych.

PLIKI WYSŁANE ZA POMOCĄ KOMUNIKATORÓW

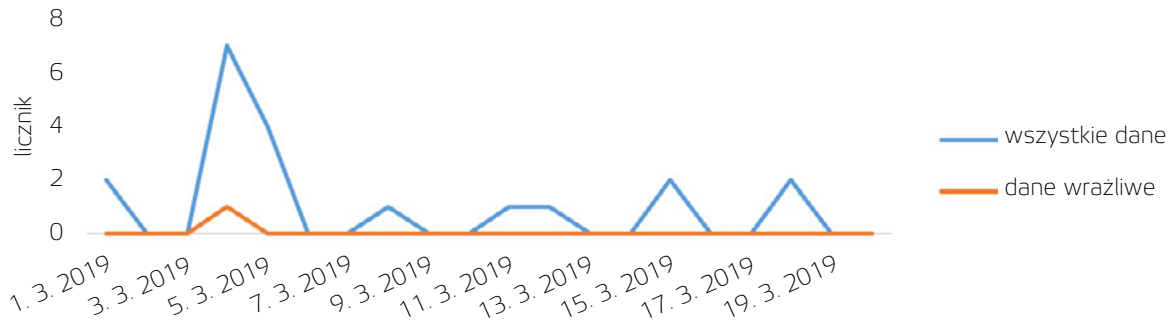
Komunikatory są narzędziem wykorzystywanym przez współpracowników i partnerów na całym świecie. Kiedy przesyłanie plików jest ograniczone do niewielkiego grona odbiorców komunikatory mogą stanowić poważne zagrożenie bezpieczeństwa, kiedy nie są kontrolowane.

18 plików zostało przesłanych przez komunikatory. Twoja polityka bezpieczeństwa nie była restrykcyjna.

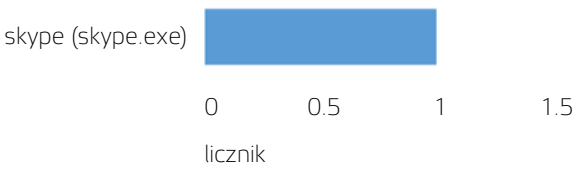
Przesyłanie plików firmowych bez żadnych ograniczeń poprzez komunikatory może narażać firmę na poważne niebezpieczeństwo.

1 wrażliwych plików z 2 plików zostało przesłanych przez komunikatory. Te pliki były zgodne z polityką bezpieczeństwa.

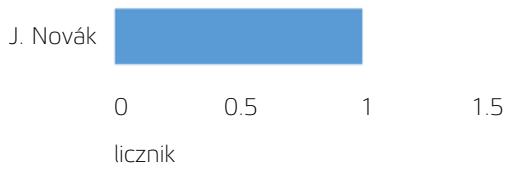
Kiedy wysłano pliki?



Gdzie przesyłano wrażliwe pliki?



Kto przesłał najwięcej wrażliwych plików?



Zalecenia:

- Sprawdź, które pliki są przesyłane. Oceń, czy pliki nie powinny być sklasyfikowane jako wrażliwe.
- Ustaw reguły DLP dla wrażliwych plików przesyłanych przez komunikatory.

PLIKI PRZESŁANE NA DYSKI CHMUROWE

Pliki firmowe mogą wyciec w przypadku przesłania na prywatne dyski chmurowe, które nie posiadają wystarczających zabezpieczeń.

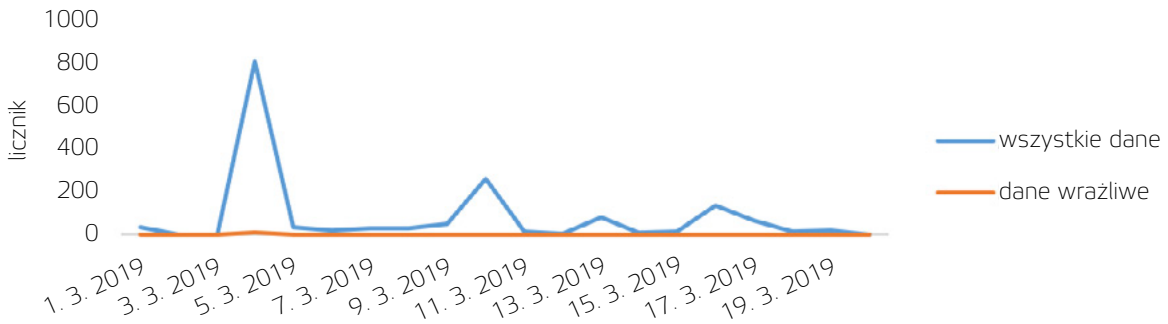
21 plików zostało przesłanych przez usługa przechowywania plików w chmurze. Te pliki nie były kontrolowane przez jakąkolwiek politykę bezpieczeństwa.

Korzystanie z prywatnych lub nieautoryzowanych dysków chmurowych stanowi poważne zagrożenie bezpieczeństwa firmowych danych.

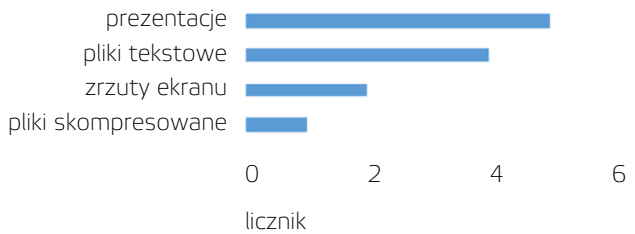
10 wrażliwych plików z 678 plików zostało przesłanych przez usługa przechowywania plików w chmurze. Twoja polityka bezpieczeństwa nie była restrykcyjna.

2 wrażliwych plików z 929 plików zostało przesłanych przez usługa przechowywania plików w chmurze. Te pliki były zgodne z polityką bezpieczeństwa.

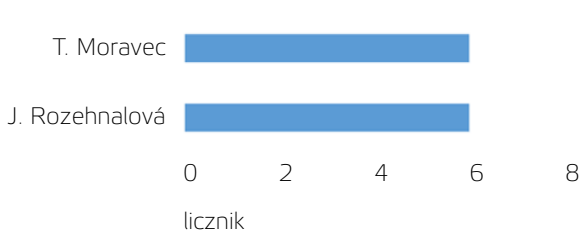
Kiedy wysłano pliki?



Jakie kategorie wrażliwych plików były przesyłane?



Kto przesłał najwięcej wrażliwych plików?



Zalecenia:

- Sprawdź jakie pliki są przenoszone. Zweryfikuj, czy któreś pliki powinny być sklasyfikowane jako wrażliwe.
- Ustaw reguły DLP dla wrażliwych plików przesyłanych na dysk chmurowy.
- Ogranicz korzystanie z dysków chmurowych, które nie są wymagane w firmie.

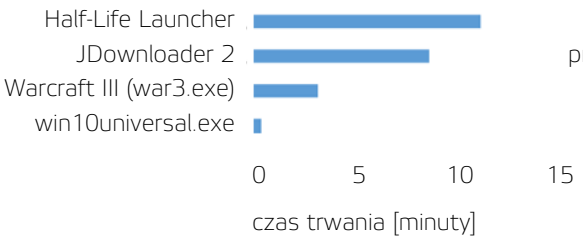
ANALIZA SPOSOBU KORZYSTANIA Z APLIKACJI

Zrozumienie, z jakich aplikacji korzystają pracownicy, pomaga firmom odkryć, gdzie mogą wystąpić zagrożenia bezpieczeństwa, a także czy zakupione licencje są wykorzystywane oraz w jaki sposób koszty i praca mogą zostać zoptymalizowane.

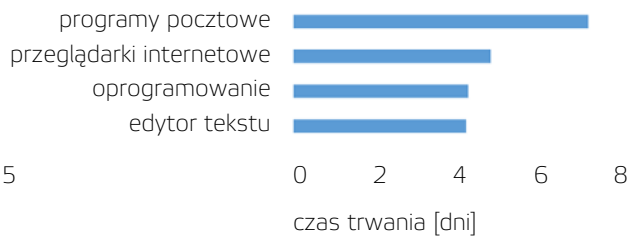
Ograniczyłeś korzystanie z ryzykownych aplikacji, które nie mogą być wykorzystywane przez pracowników.

Wyraźnie zdefiniowane zasady korzystania z aplikacji znacząco zwiększają bezpieczeństwo firmy.

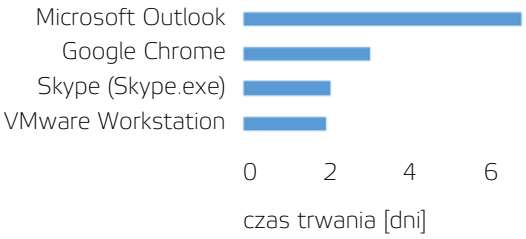
Jakie były najczęściej występujące niebezpieczne aktywności?



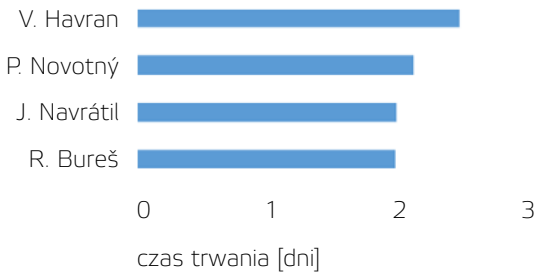
Jak pracownicy wykorzystywali czas pracy?



Jakie były najpopularniejsze aktywności użytkowników?



Aktywność użytkowników?



Zalecenia:

- Sprawdź, jakie aplikacje są wykorzystywane. Oceń, czy kategorie aplikacji wymagają modyfikacji.
- Ustaw reguły aplikacji, aby zapobiec korzystaniu z szkodliwego oprogramowania.
- Ustaw regularne automatyczne raporty dotyczące korzystania z aplikacji.

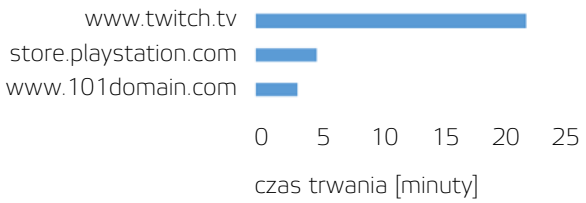
ANALIZA KORZYSTANIA Z INTERNETU

Zrozumienie, które witryny są odwiedzane przez pracowników, pomaga firmom odkryć, gdzie mogą wystąpić zagrożenia bezpieczeństwa lub w jaki sposób poprawić wydajność pracy.

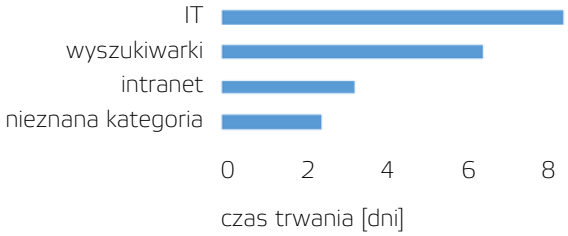
Ograniczyłeś korzystanie z ryzykownych stron internetowych, które nie mogą być odwiedzane przez pracowników.

Wyraźnie zdefiniowane zasady korzystania z stron internetowych znacząco zwiększają bezpieczeństwo firmy.

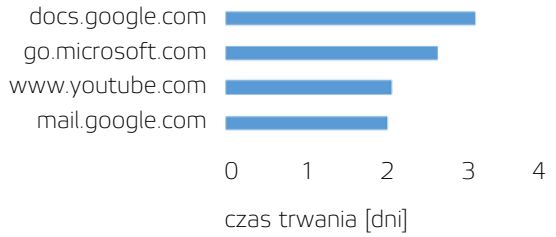
Jakie były najczęstsze ryzykowne aktywności?



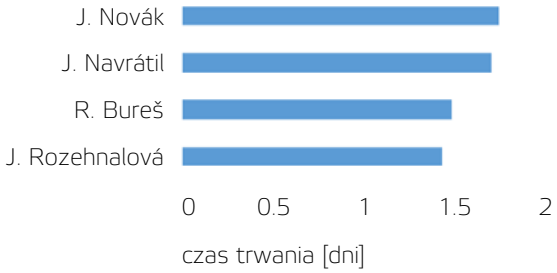
Jak pracownicy wykorzystywali czas pracy?



Jakie były najpopularniejsze aktywności użytkowników?



Aktywność użytkowników?



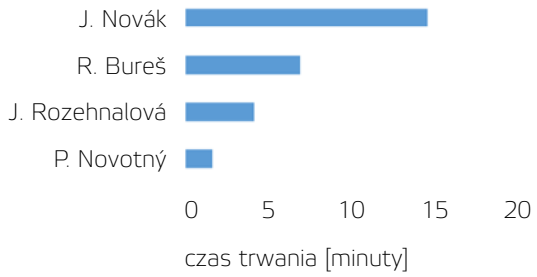
Zalecenia:

- Sprawdź, jakie witryny są odwiedzane. Oceń, czy kategorie stron internetowych wymagają modyfikacji.
- Ustaw reguły stron internetowych, aby zapobiec odwiedzaniu stron ryzykownych.
- Ustaw regularne automatyczne raporty dotyczące korzystania z stron internetowych.

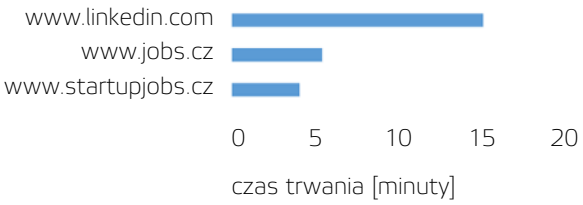
ANALIZA WYKORZYSTANIA PORTALI DO POSZUKIWANIA PRACY

Pracownicy, którzy decydują się aby opuścić firmę, mogą stanowić poważne zagrożenie bezpieczeństwa. Jeśli zabiorą ważne dokumenty i rozpoczną współpracę z konkurencją, strata dla firmy może być znacząca.

Aktywność użytkowników?



Jakie były najczęstsze aktywności?



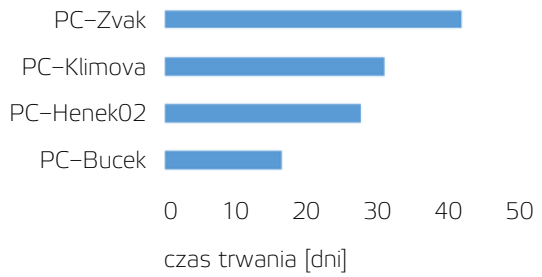
Zalecenia:

- Sprawdź, które portale do poszukiwania pracy są odwiedzane. Oceń, czy wykorzystywane kategorie stron internetowych wymagają modyfikacji.
- Ustaw powiadomienie e-mail informujące o długim czasie spędzonym na stronach poświęconych szukaniu pracy.

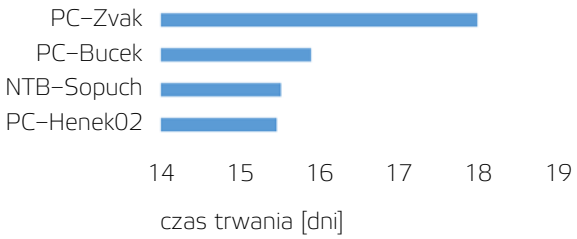
WYKORZYSTANIE ZASOBÓW – KOMPUTERY

Efektywne wykorzystanie komputerów firmowych jest ważne do ustalenia możliwych oszczędności.

Czas wykorzystywania urządzenia



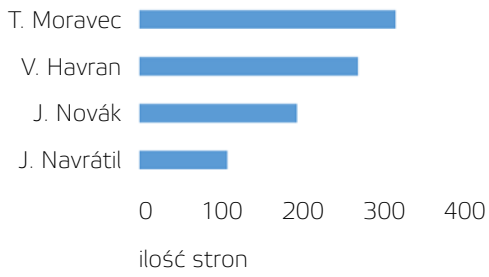
Które komputery były najczęściej bezczynne?



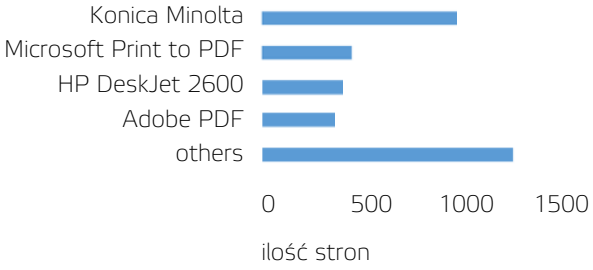
WYKORZYSTANIE ZASOBÓW – DRUKOWANIE

Raport wydruków pomoże zrozumieć, czy drukowane dokumenty stanowią naruszenie bezpieczeństwa firmy lub narażają ją na niepotrzebne koszty.

Użytkownicy korzystający z drukarek



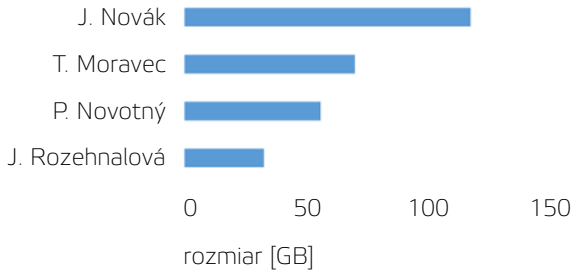
Drukarki



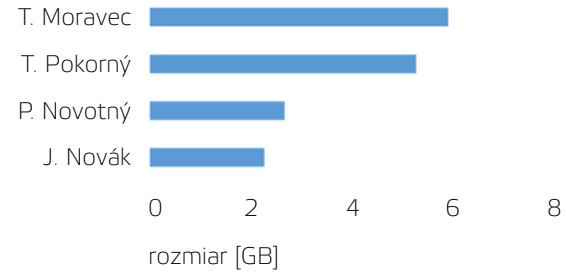
WYKORZYSTANIE ZASOBÓW – RUCH SIECIOWY

Przeładowanie lub wysyłanie dużej ilości danych przez sieć może stanowić zagrożenie dla bezpieczeństwa firmy lub wpływać negatywnie na wydajność innych pracowników.

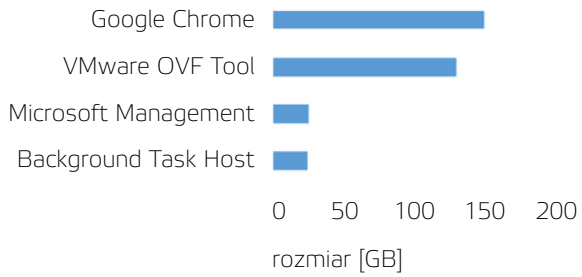
Pobieranie plików



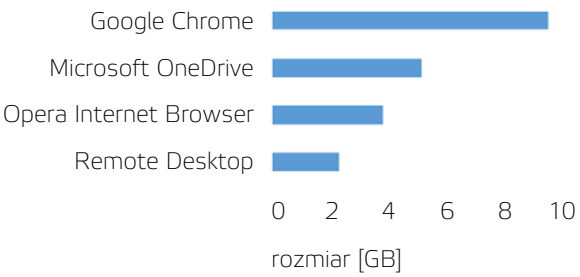
Przesyłanie plików



Pobieranie aplikacji



Przesyłanie aplikacji



O FIRMIE SAFETICA

Safetica Technologies to producent oprogramowania chroniącego przed wyciekiem danych, adresowanego do firm. Safetica ma swoją siedzibę w Republice Czeskiej. Kluczową dla Safetica wartością jest przekonanie, że każda firma zasługuje by jej dane były bezpieczne.

170 000+ chronionych urządzeń

1 400+ zadowolonych klientów

95+ krajów

70+ ekspertów bezpieczeństwa

PARTNERZY TECHNOLOGICZNI

ESET ENJOY SAFER TECHNOLOGY™

Microsoft

FORTINET Fabric-Ready

NAGRODY I OSIĄGNIECIA

Gartner

RED HERRING EUROPE WINNER 100

SC MAGAZINE AWARDS WINNER Honored in the U.S.

CYBER SECURITY EXCELLENCE AWARDS WINNER 2019

Info Security Products Guide 2019 GLOBAL EXCELLENCE BRONZE

A co z twoim danymi?

Wypróbuj rozwiązania Safetica!

safetica®