Kraków, 25.05.23

Projekt 1G1
Implementacja systemu informatycznego z zabezp. danych

Julia Sadecka, Jakub Augustyn, Beniamin Jankowski

Polityka Bezpieczeństwa v. 1.0.0

Słownik:

Administrator danych - osoba ustalająca, w jakim celu dane są przetwarzane oraz dbająca o prawidłowość procesów przebiegających w systemie i wykrywająca nadużycia.

Administrator merytoryczny - osoba posiadająca odpowiednie kwalifikacje, będąca konsultantem w kwestii wprowadzenia systemu, nadająca uprawnienia i role w systemie

Administrator techniczny - osoba posiadająca odpowiednie kwalifikacje odpowiedzialna za zarządzanie i utrzymanie infrastruktury technicznej w firmie.

Polityka bezpieczeństwa - formalny dokument, który określa zasady, wytyczne i procedury dotyczące zarządzania, ochrony i rozpowszechniania aktywów firmy.

Stanowisko obsługi danych RAW - miejsce, gdzie odbywa się przetwarzanie danych audio-wideo. Stanowisko obsługi może zawierać odpowiedni sprzęt, oprogramowanie oraz odpowiednie zasoby

Urządzenie RAW - - urządzenie służące do zbierania i zapisu danych audio-wizualnych. Jest to każdy sprzęt, który umożliwia zapis surowych danych wideo lub audio

Serwer backup: komputer lub zbiór komputerów przechowujący kopię zapasową danych

Materiał audio-video - materiał zebrany w wyniku działania kamer

I. Wprowadzenie

1. Wstęp

Niniejszy dokument, zwany również “Polityką Bezpieczeństwa” systemu audio-wideo

„RAW” firmy „Ochrona” ściśle określa zasady i wytyczne dotyczące bezpieczeństwa specjalistycznego systemu audio-wizualnego RAW. System ten umożliwia zdalny dostęp do materiałów, takich jak nagrania i filmy.

Polityka bezpieczeństwa określa takie zasady jak uprawnienia do przetwarzania danych dostępu oraz wymagane metody uwierzytelniania, obejmując zarówno aspekty techniczne, jak i organizacyjne tj. procedury odbierania uprawnień.

Głównym założeniem dokumentu jest zapewnienie oraz ochrona poufności, integralności i dostępności danych, a także minimalizowanie ryzyka wystąpienia incydentów bezpieczeństwa związanych z działaniem systemu rejestrującego dane.

Autor zastrzega prawo do wszelkich zmian polityki bezpieczeństwa, ze względu na obowiązujące przepisy oraz wszelkie zmiany występujące w infrastrukturze

2. Opis systemu

a. System

Zbiór narzędzi oraz zasobów wchodzących w skład infrastruktury monitorującej, oraz magazynującej dane zebrane przez rejestratory RAW

b. W skład systemu wchodzą:

- kamery i rejestratory RAW (zbieranie danych audiowizualnych)
- nośniki danych (zapis danych, udostępnianie najnowszych materiałów na żądanie służb)
- komputery i serwery (zarządzanie w czasie rzeczywistym)
- oprogramowanie
- interfejsy, złącza, akcesorie (łączność między magazynem danych a rejestratorami)
- magazyn sprzętu (np. zapasowe kamery)
- serwery kopii zapasowej (tzw. backup)

c. Cel powstania systemu

Monitorowanie, reagowanie oraz analiza wydarzeń oraz incydentów w firmie. Format RAW niesie ze sobą wiele korzyści, jak np. pełna kontrola kolorów, korekcja balansu bieli oraz bezstratna kompresja danych. W związku z tym, w przypadku incydentu bezpieczeństwa zebrane dane audiowizualne mogą służyć jako źródło informacji w celach dochodzenia. Zapewnia to najwyższa jakość zapisywanego obrazu, a także elastyczność w manipulowaniu nim bez obawy o utratę jakości nagrań.

3. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień oraz wskazanie osoby odpowiedzialnej za te czynności

a. **Administrator merytoryczny** odpowiada za nadawanie uprawnień i definiowanie ról w systemach. Ma za zadanie wybrać administratora danych osobowych, administratora technicznego oraz administratora RAW. Po

zaakceptowanym wyborze w systemie zostają wypełnione odpowiednie zmiany i niezbędna dokumentacja.

b. **Administrator danych** odpowiada za utrzymywanie i kontrolę bezpieczeństwa danych. Ma za zadnie chronić dostęp, szkolić pracowników, przestrzegać polityki bezpieczeństwa, monitorować system w celu wykrycia incydentów bezpieczeństwa, nadzorować procesy występujące w systemie, a także utrzymać zgodności z obowiązującymi przepisami dotyczącymi ochrony danych osobowych.

c. **Administrator techniczny** odpowiada w infrastrukturze systemu RAW za takie rzeczy jak konfiguracja, instalacja i utrzymanie sprzętu. Do jego zadań należy wdrażanie oprogramowania i aktualizacji, reagowanie na incydenty bezpieczeństwa oraz wsparcie techniczne, zarządzanie tworzeniem kopii zapasowej bazy danych

4. Procedury odbierania uprawnień do przetwarzania danych oraz wskazanie osoby odpowiedzialnej za te czynności

a. W celu odebrania uprawnień należy złożyć wniosek wraz z uzasadnieniem, który akceptuje administrator merytoryczny.

b. Administrator merytoryczny jest odpowiedzialny za dogłębną analizę informacji zawartych we wniosku o odbiór uprawnień oraz decyzję w ww. sprawie

Jeśli wniosek zostanie odrzucony:

Po udzieleniu niezbędnych wyjaśnień oraz komentarzy administrator merytoryczny może zalecić środki naprawcze

Jeśli wniosek zostanie zaakceptowany:

pracownik, o którym mowa we wniosku traci część lub całość uprawnień. Zostaje o tym natychmiast poinformowany

Instrukcja zarządzania systemem v 1.0.0

Słownik:

Administrator danych - osoba ustalająca, w jakim celu dane są przetwarzane oraz dbająca o prawidłowość procesów przebiegających w systemie i wykrywająca nadużycia.

Administrator merytoryczny - osoba posiadająca odpowiednie kwalifikacje, będąca konsultantem w kwestii wprowadzenia systemu, nadająca uprawnienia i role w systemie

Administrator techniczny - osoba posiadająca odpowiednie kwalifikacje odpowiedzialna za zarządzanie i utrzymanie infrastruktury technicznej w firmie.

Polityka bezpieczeństwa - formalny dokument, który określa zasady, wytyczne i procedury dotyczące zarządzania, ochrony i rozpowszechniania aktywów firmy.

Stanowisko obsługi danych RAW - miejsce, gdzie odbywa się przetwarzanie danych audio-wideo. Stanowisko obsługi może zawierać odpowiedni sprzęt, oprogramowanie oraz odpowiednie zasoby

Urządzenie RAW - - urządzenie służące do zbierania i zapisu danych audio-wizualnych. Jest to każdy sprzęt, który umożliwia zapis surowych danych wideo lub audio

Serwer backup: komputer lub zbiór komputerów przechowujący kopię zapasową danych

Materiał audio-video - materiał zebrany w wyniku działania kamer

I. Wprowadzenie

1. Wstęp.

Niniejszy dokument, zwany również "Instrukcją", dotyczy zarządzania systemem audio-wideo "RAW" wykorzystywanym w firmie "Ochrona". System ten jest wykorzystywany do rejestracji materiału audio-wideo za pomocą kamer nasobnych, które są noszone przez ochroniarzy wykonujących swoje obowiązki służbowe.

System kamer nasobnych składa się z różnych elementów, takich jak kamery nasobne, stacje dokujące, macierz dyskowa/serwer, serwer backup, komputery zarządzające materiałami z serwerów, stanowiska obsługi danych RAW oraz komputery zarządzające

ewidencją pobierania kamer nasobnych. Dodatkowo, istnieje magazyn, w którym przechowywane są kamery nasobne.

Głównym celem systemu jest rejestrowanie materiału audio-wideo, który pochodzi z kamer noszonych przez ochroniarzy podczas wykonywania ich zadań. Materiał ten jest przechowywany i zarządzany na serwerach, a także udostępniany na stanowiskach obsługi danych RAW, które umożliwiają ewidencję wydawania kopii nagrań.

Celem niniejszego dokumentu jest przedstawienie instrukcji dotyczącej zarządzania systemem "RAW", wraz z uwzględnieniem odpowiednich zabezpieczeń danych oraz oceną ryzyka związanego z wykorzystaniem tego systemu.

2. Opis systemu.

System audio-wideo "RAW" jest kompleksowym rozwiązaniem technologicznym, wykorzystywanym przez firmę "Ochrona" do rejestrowania i zarządzania materiałem audio-wideo pochodzącym z kamer nasobnych noszonych przez ochroniarzy. System ten umożliwia skuteczną dokumentację działań ochrony oraz zwiększenie bezpieczeństwa zarówno pracowników, jak i obiektów chronionych.

Składniki systemu "RAW" obejmują:

1. Kamery nasobne: Są to urządzenia zamocowane na ciele ochroniarzy, które rejestrują obraz i dźwięk w czasie rzeczywistym. Kamery są wyposażone w funkcje nagrywania, przesyłania strumieniowego oraz przechowywania danych.

2. Stacje dokujące: Stanowią miejsce, w którym ochroniarze mogą dokonywać ładowania baterii kamer oraz przesyłać zgromadzony materiał audio-wideo na serwer. Stacje dokujące są również odpowiedzialne za synchronizację danych i aktualizację oprogramowania w kamerach.

3. Macierz dyskowa/serwer: Jest to centralny komponent systemu, odpowiedzialny za przechowywanie, zarządzanie i udostępnianie zgromadzonego materiału audio-wideo. Macierz dyskowa gwarantuje wysoką pojemność pamięci oraz zapewnia redundantność danych w celu minimalizacji ryzyka utraty informacji.

4. Serwer backup: Komputer lub grupa komputerów, które pełnią rolę tworzenia kopii zapasowych zgromadzonych danych. Serwer backup jest kluczowy w przypadku awarii lub uszkodzenia głównego serwera, umożliwiając przywrócenie utraconych danych.

5. Komputery zarządzające materiałami znajdującymi się na serwerach: Stanowiska obsługi danych RAW, na których pracownicy odpowiedzialni za zarządzanie i analizę zgromadzonych materiałów audio-wideo mają dostęp do zasobów systemu. Zapewniają one interfejs użytkownika umożliwiający przeglądanie, odtwarzanie, indeksowanie, wyszukiwanie i udostępnianie nagrań.

6. Magazyn z kamerami nasobnymi: Jest to fizyczne miejsce, w którym przechowywane są nieużywane kamery nasobne. Magazyn zapewnia odpowiednie warunki przechowywania i zabezpieczenia sprzętu.

7. Komputery zarządzające ewidencją pobierania kamer nasobnych: Są to komputery, na których prowadzona jest kontrola i monitorowanie wypożyczeń oraz zwrotów kamer nasobnych. Zapewniają one aktualną i dokładną ewidencję wydawanych i zwracanych urządzeń.

Celem powstania systemu "RAW" jest umożliwienie rejestrowania działań ochrony za pomocą kamery noszonej przez ochroniarzy.Dane z nagrań przetwarzanych w ramach RAW można wykorzystywać do celów dydaktycznych, szkoleniowych (po ich uprzedniej anonimizacji) oraz dowodowych. Dzięki systemowi "RAW" firma "Ochrona" może zapewnić lepsze bezpieczeństwo, dokładniejszą dokumentację i skuteczną analizę sytuacji, co przekłada się na wyższy poziom usług świadczonych przez firmę.

- **Zawrzeć czym jest system**
- **Z jakich elementów system się składa. (rysunek -graf)**
- **W jakim celu powstał system..**
- **Opis poszczególnych elementów systemu:**

2.1. urządzenie audiowizualne służące do rejestrowania zdarzeń (obrazu i dźwięku) – kamera nasobna z Systemem Rejestracji Audio-Video RAW

Niewielka kamera nasobna z Systemem RAW Hikvision DS-MH2311 przypomina wyglądem aparaty GoPro. Pozwalają na nagrywanie materiałów w czasie rzeczywistym w Full HD. Kamery te mają funkcję symultanicznego strumieniowania obrazu w czasie rzeczywistym dzięki wbudowanemu kanałowi WiFi. Urządzenie może nagrywać ciągiem filmy do 8 godzin, co wystarcza na jeden dzień pracy funkcjonariusza.

Format RAW jest powszechnie stosowany w rejestrowaniu danych audiowizualnych ze względu na bezstratną kompresję. Łatwa obróbka daje większą kontrolę nad obrazem dzięki przechowywanym informacjom odnośnie kolorów, balansu bieli

2.2 aplikacja do przetwarzania danych RAW –

W systemie "RAW" używana jest zaawansowana aplikacja do przetwarzania danych w formacie RAW - Raw Therapee 5.7. Oprogramowanie to zostało specjalnie dostosowane do potrzeb firmy "Ochrona" i umożliwia efektywne zarządzanie, edycję oraz analizę zgromadzonych materiałów audiowizualnych.

Rola i zadania oprogramowania:

- Przetwarzanie danych - oprogramowanie umożliwia import i przetwarzanie danych w formacie RAW.
- Edycja - aplikacja może poprawiać jakość obrazu zmieniając kontrast czy ostrość. Co ważne nie może zmienić logiki nagrania.
- Synchronizacja audio-wideo - dokładne dopasowanie dźwięku i obrazu
- Eksport i udostępnienie - RawTherapee umożliwia eksport zgromadzonych nagrań w formatach takich jak MP4, AVI, TIFF. Oprogramowanie umożliwia także udostępnianie nagrań w celu monitoringu czy archiwizacji

2.3 stanowisko obsługi danych RAW (komputer)

Stanowisko do obsługi danych w systemie to specjalnie skonfigurowany komputer a także serwer przechowujący te dane. Na stanowisku tym wykorzystuje się specjalistyczne oprogramowanie i narzędzia do efektywnej manipulacji i analizy zgromadzonych materiałów.

Opis techniczny komputera Dell Precision 5820 Tower:

- Procesor: Intel Xeon W-2123 (4 rdzenie, 8 wątków)
- Pamięć RAM: 32 GB DDR4
- Dysk twardy: SSD NVMe 512 GB
- Karta graficzna: NVIDIA Quadro P2000 (5 GB pamięci VRAM)
- System operacyjny: Windows 10 Professional
- Specjalistyczne oprogramowanie do przetwarzania i analizy danych RAW

Opis techniczny serwera Dell PowerEdge R740:

- Procesor: Intel Xeon Silver 4210 (10 rdzeni, 20 wątków)
- Pamięć RAM: 64 GB DDR4
- Pojemność dysku: RAID 5 z 4 dyskami SAS 2 TB
- System operacyjny: Windows Server 2019
- Zainstalowane oprogramowanie do zarządzania i przechowywania danych RAW

Rola i zadania stanowiska:

- Przetwarzanie danych - za pomocą programu (opisanego w pkt 2.2) zainstalowanego na komputerze przetwarzane są dane audio-wizualne, przy których można dokonać operacji korekcji.
- Magazynowanie danych - za pomocą serwera dane są gromadzone na dyskach twardych, w celu ewentualnej ewidencji
- Ewidencja - Stanowisko umożliwia prowadzenie ewidencji nagrań (przy czym są rejestrowane informacje dotyczące pobierania, przetwarzania czy wydawania kopii nagrań)
- Archiwizacja - dane po pewnym czasie są archiwizowane, w celu zachowania historii i dostępności materiałów

3. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień oraz wskazanie osoby odpowiedzialnej za te czynności.

a) Administrator danych:

Uprawnienia i zadania:

1. Ustala cele przetwarzania danych
2. Nadzoruje prawidłowości procesów w systemie
3. Posiada pełen dostęp do wszystkich funkcji systemu tj. zarządzanie uprawnieniami użytkowników, definiowanie polityki bezpieczeństwa

Sposób nadawania uprawnień:

1. Przez administratora merytorycznego
2. Po wcześniejszej weryfikacji i autoryzacji

b) Administrator merytoryczny

Uprawnienia i zadania:

1. Konsultant w kwestii wprowadzenia systemu "RAW"
2. Nadaje uprawnienia i role w systemie (zgodnie z procedurami i zasadami)
3. Wybór administratora danych i administratora technicznego

Sposób nadawania uprawnień:

1. Przez zarząd
2. Po wcześniejszej weryfikacji i autoryzacji

c) Administrator techniczny

Uprawnienia i zadania:

1. Zarządzanie infrastrukturą techniczną
2. Monitorowanie i rozwiązywanie problemów technicznych w systemie
3. Posiada pełen dostęp do narzędzi
4. Posiada dostęp do uprawnień koniecznych do skutecznego zarządzania sprzętem, oprogramowaniem i zabezpieczeniami

Sposób nadawania uprawnień:

3. Przez administratora merytorycznego
4. Po wcześniejszej weryfikacji i autoryzacji

Procedura nadawania uprawnień:

1) Weryfikacja tożsamości i uprawnień
2) Określenie roli i uprawnień, które uzyska dana osoba
3) Dokumentacja wszystkich uprawnień w systemie
4) Regularne przeglądy i audyty nadanych uprawnień

4. Procedury odbierania uprawnień do przetwarzania danych i rejestrowania tych uprawnień oraz wskazanie osoby odpowiedzialnej za te czynności.

a) Administrator Danych

Odebranie:

1. Przez administratora merytorycznego
2. Po wcześniejszej weryfikacji i autoryzacji
3. Po odebraniu traci dostęp do wszystkich funkcji systemu opisanymi w pkt. 3

b) Administrator merytoryczny

Odebranie:

1. Przez zarząd, włączając w to administratora danych
2. Po odebraniu uprawnień, traci możliwość nadawania uprawnień i zarządzania rolami w systemie.

c) Administrator techniczny

Odebranie:

1. Przez administratora merytorycznego
2. Po wcześniejszej weryfikacji i autoryzacji
3. Traci dostęp do narzędzi i funkcji umożliwiających zarządzanie infrastrukturą techniczną

Procedura odebrania uprawnień:

1) W celu odebrania uprawnień należy złożyć wniosek wraz z uzasadnieniem, który akceptuje administrator merytoryczny.
2) Administrator merytoryczny jest odpowiedzialny za dogłębną analizę informacji zawartych we wniosku o odbiór uprawnień oraz decyzję w ww. sprawie

- **Jeśli** wniosek zostanie odrzucony:

  Po udzieleniu niezbędnych wyjaśnień oraz komentarzy administrator merytoryczny może zalecić środki naprawcze

- **Jeśli** wniosek zostanie zaakceptowany:

  Pracownik, o którym mowa we wniosku traci część lub całość uprawnień. Zostaje o tym natychmiast poinformowany

5. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem.

5.1. Zasady dotyczące haseł.

Ogólne zasady dotyczące haseł:
- przetrzymywanie w postaci hash (zalecany: SHA256)
- ograniczona ilość prób logowania - po 5 próbach następuje zablokowanie konta
- hasło nie może być słownikowe (przykładowy słownik: *rockyou.txt*)
- hasło nie może się powtórzyć na przestrzeni roku

Wymagania dotyczące hasła **użytkownika RAW:**
- długość - zakres od 10 do 64 znaków
- poziom skomplikowania - litera duża oraz mała, znak specjalny
- aktualizacja - raz na trzy miesiące
- odblokowanie konta po prośbie napisanej do administratora danych
- możliwość weryfikacji dodatkowym składnikiem (kod SMS lub z aplikacji)

Wymagania dotyczące hasła **administratora technicznego i administratora RAW:**
- długość - zakres od 14 do 64 znaków
- poziom skomplikowania - litera wielka, mała, cyfra, znak specjalny
- aktualizacja - raz na miesiąc
- **wymagane** uwierzytelnianie wieloskładnikowe (kod SMS lub aplikacji, zalecany klucz fizyczny YUBIKEY)
- w przypadku konieczności resetowania hasła wymagane rygorystyczne uwierzytelnianie

6. Procedury rozpoczęcia, zawieszenia i zakończenia pracy na stanowisku obsługi danych RAW.

Celem procedury jest zabezpieczenie danych osobowych przed nieuprawnionym dostępem i utratą poufności w sytuacji, gdy użytkownik RAW i administrator RAW rozpoczyna, przerywa lub kończy pracę na stanowisku obsługi danych RAW.
Aplikację RAW na stanowisku komputerowym obsługuje administrator RAW. W przypadku, gdy administrator danych RAW jest jednocześnie użytkownikiem RAW, czynności administracyjne wobec zarejestrowanego przez niego materiału AV realizuje inny wyznaczony administrator RAW.

6.1 Użytkownik RAW.

a) Rozpoczęcie pracy

1. Zaloguj się na swoje konto użytkownika RAW, korzystając z indywidualnych danych uwierzytelniających.
2. Sprawdź, czy wszystkie niezbędne urządzenia są podłączone i działają poprawnie.
3. Upewnij się, że masz odpowiednie uprawnienia do wykonywania swoich obowiązków na stanowisku obsługi danych RAW.

b) Wykonywanie czynności

1. Przeglądaj, edytuj i analizuj zgromadzone materiały audiowizualne zgodnie z obowiązującymi zasadami i procedurami.
2. Dokonuj niezbędnych zapisów, ewidencji i rejestracji dotyczących obsługiwanych danych RAW.
3. W razie wykrycia jakichkolwiek nieprawidłowości, problemów technicznych lub naruszeń bezpieczeństwa, niezwłocznie zgłoś to odpowiedniej osobie, takiej jak administrator RAW.

c) Zawieszenie pracy

1. Jeśli musisz przerwać pracę na stanowisku obsługi danych RAW na krótki okres, upewnij się, że wszystkie urządzenia są bezpieczne i chronione przed nieuprawnionym dostępem.
2. Zapisz bieżącą pracę i zamknij wszystkie aktywne projekty.
3. Zablokuj swoje konto użytkownika lub wykonaj inne odpowiednie procedury zabezpieczające zgodnie z polityką bezpieczeństwa organizacji.

d) Zakończenie pracy

1. Zapisz i zamknij wszystkie otwarte aplikacje i programy związane z obsługą danych RAW.
2. Zakończ sesję na swoim koncie użytkownika i wyloguj się z systemu.
3. Upewnij się, że wszystkie urządzenia są bezpieczne, a stanowisko obsługi danych RAW jest odpowiednio zabezpieczone przed nieuprawnionym dostępem.

6.2 Administrator RAW.

a) Rozpoczęcie pracy

1. Zaloguj się na swoje konto administratora RAW, korzystając z indywidualnych danych uwierzytelniających.
2. Sprawdź, czy wszystkie niezbędne urządzenia są podłączone i działają poprawnie.
3. Upewnij się, że masz odpowiednie uprawnienia do wykonywania swoich obowiązków na stanowisku obsługi danych RAW.

b) Wykonywanie czynności

1. Nadzoruj i zarządzaj dostępem użytkowników RAW do materiałów audiowizualnych zgodnie z polityką bezpieczeństwa organizacji.
2. Przeglądaj, edytuj i analizuj zgromadzone materiały audiowizualne zgodnie z obowiązującymi zasadami i procedurami.
3. Prowadź działania administracyjne wobec zarejestrowanych przez siebie materiałów AV, takie jak tworzenie kopii zapasowych, archiwizacja, kontrola jakości.

c) Zawieszenie pracy

1. Jeśli musisz przerwać pracę na stanowisku obsługi danych RAW na krótki okres, upewnij się, że wszystkie urządzenia są bezpieczne i chronione przed nieuprawnionym dostępem.
2. Zablokuj swoje konto administratora lub wykonaj inne odpowiednie procedury zabezpieczające zgodnie z polityką bezpieczeństwa organizacji.

d) Zakończenie pracy

1. Zapisz i zamknij wszystkie otwarte aplikacje i programy związane z obsługą danych RAW.
2. Zakończ sesję na swoim koncie administratora i wyloguj się z systemu.
3. Upewnij się, że wszystkie urządzenia są bezpieczne, a stanowisko obsługi danych RAW jest odpowiednio zabezpieczone przed nieuprawnionym dostępem.

7. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

Użyte środki:

1. System kopii zapasowej danych
   - Wykorzystywane oprogramowanie: Backup Exec 21.2.
   - Opis oprogramowania: zaawansowane narzędzie do tworzenia kopii zapasowych danych. Automatycznie tworzy kopię zapasową wszystkich rodzajów danych. Umożliwia przywrócenie danych w przypadku awarii

2. Magazyn danych dla kopii zapasowych
   - Wykorzystane narzędzie: Zewnętrzny dysk twardy o pojemności 10 TB.
   - Opis narzędzia: Zewnętrzny dysk o dużej pojemności służy jako magazyn danych dla kopii zapasowych. Dysk zapewnia szybki dostęp do kopii zapasowych

Procedura tworzenia kopii zapasowych:

1) Określenie harmonogramu - Administrator systemu ustala harmonogram tworzenia kopii zapasowych (częstotliwość i godzina)
2) Konfiguracja oprogramowania
   - konfiguracja Backup Exec
   - zdefiniowanie źródeł danych do kopii zapasowych
   - wybranie odpowiednich ustawień (szyfrowanie)
3) Wykonanie kopii zapasowych
4) Monitorowanie i weryfikacja - Administrator powinien regularnie monitorować proces tworzenia kopii zapasowych w celu sprawdzenia poprawności wykonania, weryfikacji spójności i integralności skopiowanych danych
5) Przechowywanie kopii zapasowych - należy dopasować miejsce przechowywania do rodzajów dysku (zabezpieczone miejsce, odpowiednia temperatura)

8. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

a) Odstępy czasowe dla przeglądów oraz konserwacji sprzętu i nośników

- wymagane jest, aby stosować się do zaleceń producenta danego sprzętu, co ma stanowić podstawę do wyznaczenia okresu między przeglądami sprzętu oraz nośników, a także określenie przedziału czasu dla konserwacji danego sprzętu. Przeglądy i konserwacje należy przeprowadzać nie rzadziej niż zalecenia opisane właśnie przez producenta.

- W przypadku niejasnych lub całkowitemu braku tego typu zaleceń, sprawę należy przekierować do administratora technicznego, który to sam określi dane okresy czasu dla poszczególnych sprzętów.

b) Przypadek wykrycia usterki (m. in. podczas przeglądu)

- W przypadku wykrycia usterki, należy przekazać sprzęt/nośnik do administratora technicznego, który miarę możliwości, tzn. kompetencji oraz posiadanym wyposażeniem, ma obowiązek naprawić niedziałające funkcje.

- Należy pamiętać o pełnej dokumentacji danej sprawy naprawczej - kluczowym jest podanie terminów oraz wskazanie osób odpowiedzialnych za przekazany sprzęt/nośnik.

- W tym punkcie zawarta jest informacja dot. naprawy nośników danych. Jeżeli nośnik danych zawierał dane osobowe osób trzecich, należy bezzwłocznie wyczyścić (sformatować) dysk w celu wymazania znalezionych informacji. W przypadku braku możliwości sformatowania dysku - sam nośnik należy zutylizować w taki sposób, aby dostęp do danych zapisany na nim, był niemożliwy.

9. Procedura kontroli dostępu i rozliczalności.

a) **Dostępność**

- Dostęp do systemu oraz zbieranych danych może być udostępniony tylko wybranym osobom, które wg administratorów. Taki dostęp mają uzyskać tylko kwalifikowani oraz upoważnieni pracownicy. Należy kontrolować i bronić dostępność do systemu osobom do tego nieupoważnionym.

b) **Integralność**

- Jest to punkt zapewniający, iż dane nie zostały w żaden sposób naruszone oraz zmodyfikowane. Należy pamiętać, aby zawsze sprawdzać integralność, np. przy tworzeniu kopii zapasowych. W tym celu, zalecane jest użycie wszelkich bezpiecznych funkcji haszujących z rodziny SHA-2 lub nowszych - SHA-3. W ten sposób zauważymy wszelkie niezgodności oraz informację o modyfikacji danego pliku/plików.

c) **Rozliczalność**

- W związku z odpowiednio przydzielonym oraz kontrolowanym dostępem, każde działania użytkowników są monitorowane. Wszelkie próby włamań/ataków zostaną wychwycone oraz powiązane z poszczególną jednostką, która zostanie ona zidentyfikowana. Celem jest m. in. wewnętrzna ochrona systemu oraz poprawne jego funkcjonowanie.

10. Archiwizacja danych.

Archiwizacja danych odbywa się w oparciu o regulacje zawarte w pkt VII „Instrukcji obsługi systemu rejestracji audio-wideo (RAW)". W związku z użyciem oprogramowania Backup Exec 21.2, sam proces archiwizacji danych jest ułatwiony:

- Należy stworzyć kopię zapasową danych, które chcemy, aby zostały poddane procesowi archiwizacji.
- Następnie należy sprawdzić integralność zebranych danych (m. in. punkt 9.).
- Jeżeli wcześniejsze punkty zostały wykonane poprawnie, można usunąć pierwotne dane.
- Dane należy trzymać przez 4 lata, po czym następuje usunięcie ich z archiwum.
- Trzymane dane w archiwum to nagrania z kamer naosobowych oraz historię ewidencji kamer

11. Udostępnianie zgromadzonych materiałów

a) Dane z kamer nasonych należy w szczególnym przekazać podmiotom tylko do tego uprawnionym. Ustalanie odbywa się na podstawie aktualnie obowiązujących przepisów prawa.

b) Po przeanalizowanie podpunktu a) - należy zweryfikować osobę, która wymaga od firmy udostępnienia nagrań z omawianych kamer lub ewentualny wgląd do kamer w czasie rzeczywistym. W tym celu wymagamy zidentyfikowania się przez osobę/podmiot, która żąda wglądu, poprzez np. legitymację służbową. Dodatkowo, fakt wystąpienia takiego wglądu należy zaznaczyć oraz odnotować.

c) Dla upoważnionych osób, istnieje możliwość zapisania danych osobowych z systemu zapisu nagrań kamer. Wymagane jest natomiast posiadania bezpiecznego nośnika, na którym takie dane może zapisać.

d) Istnieje również złożenie wniosku, który również pozwalałby na udostępnienie zebranych materiałów odpowiednim podmiotom. W tym celu należy pamiętać o bezpiecznym tunelu przesyłu danych, który spełniałby wszelkie wymogi bezpieczeństwa, w tym wymogi kryptograficzne, tj. stosowanie bezpiecznych algorytmów szyfrujących. Zgodę na takie przekazanie danych wyraża Administrator Danych.

Akceptuję

. . . . . .
(kierownik jednostki organizacyjnej)

Szacowanie ryzyka dla Systemu kamer nasobnych

(nazwa sieci)

Niniejsze szacowanie ryzyka przeprowadzono w oparciu o *„Metodę zarządzania ryzykiem dla systemów teleinformatycznych”* w wersji 1.0.

Zamieszczona poniżej macierz odzwierciedla podatności i zagrożenia zidentyfikowane w metodzie i ma na celu oszacowanie liczbowych wartości ryzyka.

Obliczane ryzyko na podstawie danego wzoru:
$R_p = P \cdot (S_d + S_i + S_p)$; gdzie:
P - prawdopodobieństwo wystąpienia
S_d - wartość przypisana skutkowi dla dostępności informacji
S_i - wartość przypisana skutkowi dla integralności informacji
S_d - wartość przypisana skutkowi dla poufności informacji

$P, S_d, S_i, S_p \in \{0, 1, 2, 3, 4\}$

Macierz Ryzyka:

Zagrożenia	Ryzyko				
	P	Sd	Si	Sp	Rp
1. Kategoria zagrożenia: Wniknięcie kodu złośliwego z sieci WAN					
1. Brak lub złe umiejscowienie w systemie lub brak aktualizacji oprogramowania typu AV	2	2	2	2	12
2. Brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja zapór sieciowych (firewall)	1	2	2	1	5
3. Brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja oprogramowania IPS/IDS i jego sond	1	2	2	1	5
4. Niewłaściwa konfiguracja mechanizmów bezpieczeństwa w sieciach WAN	2	3	2	2	14
5. Brak monitorowania obciążenia serwerów	1	0	2	0	2
6. Podatność użytkowników na oddziaływanie metod inżynierii społecznej w celu uzyskania informacji lub wprowadzenia kodu złośliwego	2	3	2	4	18
2. Kategoria zagrożenia: Wniknięcie kodu złośliwego z sieci LAN					
1. Brak lub złe umiejscowienie w systemie lub brak aktualizacji oprogramowania typu AV	2	2	2	2	12
2. Brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja zapór sieciowych (firewall)	1	2	2	1	5
3. Brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja oprogramowania IPS/IDS i jego sond	1	1	2	2	5
4. Niewłaściwa konfiguracja mechanizmów bezpieczeństwa w sieciach LAN	1	2	3	2	7
3. Kategoria zagrożenia: Atak typu DDoS lub DoS					
1. Brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja zapór sieciowych (firewall)	2	2	2	0	6
2. Brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja oprogramowania IPS/IDS i jego sond	2	2	1	0	6
3. Brak nadzoru nad ruchem sieci (QoS)	1	2	2	0	4
4. Brak monitorowania obciążenia serwerów	2	3	2	0	10
5. Błąd oprogramowania	3	3	2	0	15
6. Utrata dostępu do usług sieci WAN (w tym internetu) w wyniku ataku na komponenty sieci WAN	3	2	2	0	12
4. Kategoria zagrożenia: Nieautoryzowany dostęp do informacji					
1. Brak nadzoru nad uprawnieniami użytkowników, uprawnienia nieadekwatne do zadań	3	4	3	4	33
2. Zbyt wolne wnoszenie zmian uprawnień użytkowników	3	3	4	2	27
3. Brak kontroli dostępu fizycznego do elementów systemu	1	2	4	2	8
4. Zagubienie/zniszczenie nośnika	2	2	2	4	16
5. Nieautoryzowany dostęp pracowników serwisu do informacji	1	4	3	4	11
5. Kategoria zagrożenia: Nieumiejętne posługiwanie się systemem przez administratora					
1. Brak właściwych szkoleń administratorów w zakresie użycia systemu	3	3	2	3	24
2. Brak kontroli jakości danych wprowadzanych do systemu	1	2	3	3	8
3. Odzyskiwanie informacji z nośników wycofanych z użycia	2	4	0	4	16

4. Podatność użytkowników na oddziaływanie metod inżynierii społecznej w celu uzyskania informacji lub wprowadzenia kodu złośliwego	1	3	4	3	10
5. Odmowa realizacji zadań	1	4	0	2	6
6. Uszkodzenie urządzeń/oprogramowania w wyniku niedbalstwa (zalanie, upuszczenie)	1	1	0	0	1
7. Nieznajomość hasła/haseł administratora.	1	4	0	0	4
8. Ujawnienie hasła administratora	1	4	4	4	12
9. Rutyna i/lub nadmiar obowiązków administratora	1	4	1	2	7
10. Błędy i pomyłki w zarządzaniu systemem.	3	2	2	3	14
6. Kategoria zagrożenia: Przełamanie zabezpieczeń dostępu wewnątrz systemu					
1. Brak nadzoru nad uprawnieniami użytkowników, uprawnienia nieadekwatne do zadań (np. możliwość instalacji programów, w tym służących przełamaniu zabezpieczeń)	1	3	3	3	9
2. Zbyt wolne wnoszenie zmian uprawnień użytkowników	1	3	4	3	10
3. Brak nadzoru nad aktywnością użytkowników w systemie	2	4	3	2	18
4. Brak, złe umiejscowienie w systemie lub brak aktualizacji oprogramowania typu AV	2	3	3	2	16
5. Brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja zapór sieciowych (firewall)	2	2	2	2	12
6. Brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja 7. oprogramowania IPS/IDS i jego sond	2	3	2	2	14
7. Ujawnienie hasła administratora	1	4	4	4	12
7. Kategoria zagrożenia: Podsłuch danych, przechwyt danych					
1. Brak nadzoru nad ruchem sieci (QoS)	2	1	1	3	10
2. Emisja ujawniająca	1	2	0	3	5
3. Brak szyfrowania w łączach WAN	1	0	0	4	4
4. Podsłuch informacji w sieci wewnętrznej (LAN)	1	0	0	4	4
5. Pozyskanie informacji z nośników wycofanych z użycia	2	2	0	4	12
6. Nieuprawnione wykorzystanie/modyfikowanie urządzeń	1	2	1	4	7
7. Wykorzystanie podsłuchu programowego	3	1	1	2	4
8. Kategoria zagrożenia: Włamanie do systemu teleinformatycznego z sieci zewnętrznej WAN (przełamanie zabezpieczeń)					
1. Brak aktualizacji oprogramowania systemowego	3	2	2	2	18
2. Brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja zapór sieciowych (firewall)	2	2	3	2	14
3. Brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja oprogramowania IPS/IDS i jego sond	2	2	2	2	12
4. Brak nadzoru nad ruchem sieci (QoS)	2	3	3	2	16
5. Brak monitorowania obciążenia serwerów	1	2	2	0	4
6. Podatność użytkowników na oddziaływanie metod inżynierii społecznej w celu uzyskania informacji lub wprowadzenia kodu złośliwego	3	4	2	4	30

9. Kategoria zagrożenia: System podmiotu (urzędu)źródłem zakłóceń w cyberprzestrzeni					
1. Brak nadzoru nad ruchem sieci (QoS)	2	3	3	2	16
2. Brak lub złe umiejscowienie w systemie lub brak aktualizacji oprogramowania typu AV	2	2	2	2	12
3. Brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja zapór sieciowych (firewall)	2	2	3	2	14
4. Brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja oprogramowania IPS/IDS i jego sond	2	2	3	2	14
10. Kategoria zagrożenia: Klęski żywiołowe i katastrofy					
1. Nieprzewidywalne oddziaływanie sił natury (opady, wiatry, pioruny, ekstremalne temperatury, itp.)	0	0	0	0	0
2. Pożar	1	2	0	0	2
3. Katastrofy (budowlane, komunikacyjne, itp.)	1	2	0	0	2
11. Kategoria zagrożenia: Akty kryminalne/terroryzm					
1. Kradzież/zniszczenie urządzeń/nośników	1	3	3	4	10
2. Włamanie się fizyczne do pomieszczenia	1	2	3	3	8
12. Kategoria zagrożenia: Serwisowanie i inne czynności w systemie					
1. Nieautoryzowany dostęp pracowników serwisu do informacji	2	2	1	3	12
2. Niewłaściwe serwisowanie urządzeń/oprogramowania zamierzone lub wynikające z niedbalstwa	2	3	2	2	14
3. Kradzież urządzeń/nośników przez pracowników serwisu	2	3	2	4	18

Wnioski:

W wyniku przeprowadzenia szacowania ryzyka dla sieci monitoringu miejskiego stwierdzono, co następuje:

1. Ryzyko $R_p \leq 8$ - jest to ryzyko, które jest akceptowalne, tzn. szansa na jego wystąpienie lub ewentualne straty w związku z jego wystąpieniem są na stosunkowo niewielkie. (25 zdarzeń z 63)
2. Ryzyko $R_p > 8$ i $R_p \leq 30$ - jest to ryzyko, któremu trzeba przeciwdziałać. Należy ograniczyć jego potencjalne skutki oraz zminimalizować możliwość wystąpienia zdarzenia, które zalicza się do tej kategorii. (37 zdarzeń z 63)
3. Ryzyko $R_p > 30$ - ryzyko, które niezwłocznie trzeba zminimalizować. Dla firmy, zdarzenia należące do tej kategorii ryzyka, mogą nieść za sobą poważne konsekwencje, w tym duże konsekwencje finansowe. Zalecana natychmiastowa reakcja. (1 zdarzeń z 63)

Średnia wartość R_p wyniosła ~ 10.92.

Działania umożliwiające zwiększenie poziomu zabezpieczeń:

1. Przeprowadzanie okresowych audytów bezpieczeństwa.
2. Należy regularnie szkolić odpowiedzialne osoby za system RAW lub powiązane osoby z tym systemem pod kątem odpowiednim zarządzaniem tym systemem.
3. Należy organizować również szkolenia, które będą miały za zadanie chronić pracowników przed wpływem socjotechniki.
4. Wymuszanie zmiany haseł na użytkownikach oraz dbanie o siłę stosowanych haseł (zgodnie z punktem 8. Instrukcji zarządzania systemem).
5. Okresowe sprawdzanie sprzętu oraz naprawy (zgodnie z punktem 5.1. Instrukcji zarządzania systemem).
6. Ciągła aktualizacja kont, które mają dostęp do systemu (m. in. usuwanienie nieużywanych kont)
7. Zwiększenie poziomu redundancji urządzeń sieciowych, szczególnie szkieletowych oraz dystrybucyjnych.
8. Wdrożenie systemu zarządzania architekturą, bezpieczeństwem i autoryzacją dostępu do sieci.
9. Wdrożenie systemu monitorowania stanu i natężenia przepływu danych w sieci.

Szacowania dokonał zespół w składzie:

_____
(imię, nazwisko, stanowisko lub funkcja)

_____
(imię, nazwisko, stanowisko lub funkcja)

Wnoszę o zaakceptowanie**:

…….
administrator techniczny/
lokalny administrator techniczny*

*niepotrzebne skreślić
**(wniosek o akceptację w przypadku pkt. 2 lub 3

Ewidencja wydania/przyjęcia kamer nasobnych

p.	Nr kamery nasobnej	R odzaj moco wania	Stopień, imię i nazwisko policjanta pobierającego kamerę	Data i godzina pobrania, podpis pobierającego	Data i godzina zdania, podpis przyjmujacego	U wagi

Ewidencja przekazania materiału RAW

p	Imię i nazwisko osoby, której przekazano materiał, podpis	Rodzaj przekazanego materiału (np. szkoleniowy)	Ilość wielkość plików oraz rodzaj nośnika	Forma przekazania	Data i podpis osoby przekazującej materiał

Ewidencja uwag i usterek RAW

p	Data zgłoszenia	Imię i nazwisko osoby zgłaszającej	Rodzaj usterki /uwagi	Kogo poinformowano	Inne adnotacje
