Kraków, 17.03.23

Ocena Skutków Incydentów

Julia Sadecka, Jakub Augustyn, Beniamin Jankowski

1. W jaki sposób doszło do wycieku

Algorytm postępowania:

a. Przeprowadzić wstępną analizę, aby zrozumieć, co stało się z systemem.
b. Sprawdzić, czy serwer i oprogramowanie zostały poprawnie skonfigurowane, aby wykluczyć możliwość błędów systemowych.
c. Przeprowadzić audyt dostępu do systemu, aby zobaczyć, kto miał dostęp do systemu i kiedy.
d. Sprawdzić, czy system był narażony na atak z zewnątrz poprzez analizę logów sieciowych.
e. Sprawdzić, czy system był narażony na atak z wewnątrz poprzez analizę logów systemowych.
f. Sprawdzić, czy użytkownicy systemu stosowali się do polityk bezpieczeństwa, w tym do wymagań dotyczących haseł i autoryzacji.

Nasz przypadek:

Atakujący wykorzystał: *niezabezpieczone porty sieciowe i log4j*
Wykonał atak typu: *remote code execution*

1. Atakujący skanuje sieć w poszukiwaniu wrażliwych aplikacji
2. Atakujący odnajduje niezabezpieczony port sieciowy za pomocą narzędzia nmap, które wykrywa niezabezpieczone porty i identyfikuje usługi systemu teleinformatycznego rejestracji wideo kamer, które na nich działają.
3. Atakujący zidentyfikował lukę w log4j, popularnej bibliotece logowania, wykorzystywanej przez system rejestracji wideo. Luka ta umożliwiała wykonanie zdalnego kodu, co oznaczało, że atakujący mógł zdalnie uruchomić kod na komputerze docelowym bez konieczności uzyskiwania fizycznego dostępu do niego.
4. Dzięki luce w log4j zdalnie wykonał kod, który umożliwił mu uzyskanie dostępu do systemu rejestracji wideo. W ten sposób mógł zdalnie wykonywać komendy na zdalnym serwerze, zyskując w ten sposób pełny dostęp do systemu.
5. Po uzyskaniu dostępu do systemu atakujący mógł pobrać nagrane materiały i przesłać je na zewnętrzny serwer, poprzez protokół SSH. W tym przypadku atakujący ewentualnie mógł skonfigurować system rejestracji wideo tak, aby przekierowywał nagrania na jego własne serwery, a następnie opublikował je w Internecie.

2. W jaki sposób reagujemy na zagrożenie

Algorytm postępowania:

Po zidentyfikowaniu przyczyn wycieku administrator systemu powinien podjąć odpowiednie kroki, aby ograniczyć straty i zagrożenia dla systemu:

a. Odcięcie systemu od Internetu, aby zminimalizować ryzyko dalszego naruszania systemu przez osoby nieuprawnione.

b. Wdrożenie środków bezpieczeństwa, takich jak zwiększenie złożoności haseł, zmiana uprawnień użytkowników i poprawa konfiguracji systemu.
c. Przeprowadzenie audytu bezpieczeństwa systemu w celu zidentyfikowania słabych punktów w systemie i zapobieganie przyszłym incydentom.

Nasz przypadek:

1. Potwierdzenie naruszenia systemu: Administratorzy potwierdzają, że system rzeczywiście został zhakowany, a dane nagrane przez kamery wideo są dostępne publicznie w Internecie.
2. Odcinanie atakującego: Jeśli atakujący wciąż jest zalogowany na systemie, należy natychmiast wylogować go lub odłączyć go od sieci.

3. Dalsze kroki po zlokalizowaniu usterki

Algorytm postępowania:

a. Poinformowanie pracowników o incydencie i wyjaśnienie, jakie kroki zostały przeprowadzone, aby zapobiec przyszłym incydentom.
b. Wprowadzenie zmian w polityce bezpieczeństwa w celu zapobieganiu przyszłym incydentom.
c. Zadbanie o to, aby wszyscy użytkownicy systemu zostali poinstruowani w zakresie bezpieczeństwa i przestrzegali polityki bezpieczeństwa.

Nasz przypadek:

1. Zabezpieczenie systemu: Administratorzy wdrażają wszelkie dostępne aktualizacje zabezpieczeń, poprawki i łatki dotyczące systemu i aplikacji, aby zapobiec kolejnym atakom. Mogą też przeprowadzić audyt bezpieczeństwa systemu i zidentyfikować słabe punkty.
2. Usunięcie log4j: Jeśli aplikacje w systemie korzystają z log4j, należy zaktualizować je do wersji, w której luka została załatana, lub wyłączyć logowanie.
3. Zmiana haseł: Administratorzy powinni zmienić wszystkie hasła dostępowe do systemu i aplikacji, a także wymusić zmianę haseł dla użytkowników.
4. Powiadomienie organów: Jeśli naruszone zostały poufne informacje, administratorzy powinni powiadomić odpowiednie organy, takie jak organy nadzoru, organy ścigania lub inspektorów ochrony danych.
5. Monitorowanie systemu: Administratorzy powinni monitorować system przez okres co najmniej kilku dni, aby upewnić się, że nie ma innych naruszeń.
6. Szkolenia dla pracowników: Administratorzy powinni zorganizować szkolenia dla pracowników, aby nauczyć ich, jak unikać ataków i jak reagować w przypadku podejrzenia naruszenia.

4. Macierz 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

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

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**	**3**	**2**	**7**
3. Brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja oprogramowania IPS/IDS i jego sond	**2**	**2**	**1**	**2**	**10**
4. Niewłaściwa konfiguracja mechanizmów bezpieczeństwa w sieciach WAN	**1**	**3**	**2**	**2**	**7**
5. Brak monitorowania obciążenia serwerów	**1**	**0**	**1**	**0**	**2**
6. Podatność użytkowników na oddziaływanie metod inżynierii społecznej w celu uzyskania informacji lub wprowadzenia kodu złośliwego	**3**	**3**	**2**	**4**	**27**
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**	**1**	**0**	**1**	**2**
3. Brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja oprogramowania IPS/IDS i jego sond	**2**	**2**	**1**	**2**	**10**
4. Niewłaściwa konfiguracja mechanizmów bezpieczeństwa w sieciach LAN	**3**	**2**	**2**	**2**	**18**
3. Kategoria zagrożenia: Atak typu DDoS lub DoS					
1. Brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja zapór sieciowych (firewall)	**3**	**3**	**2**	**0**	**15**

2. Brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja oprogramowania IPS/IDS i jego sond	**2**	**4**	**2**	**0**	**12**
3. Brak nadzoru nad ruchem sieci (QoS)	**2**	**3**	**2**	**0**	**10**
4. Brak monitorowania obciążenia serwerów	**1**	**3**	**2**	**0**	**5**
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	**4**	**3**	**4**	**2**	**36**
3. Brak kontroli dostępu fizycznego do elementów systemu	**1**	**2**	**4**	**2**	**8**
4. Zagubienie/zniszczenie nośnika	**2**	**3**	**2**	**5**	**20**
5. Nieautoryzowany dostęp pracowników serwisu do informacji	**3**	**4**	**3**	**4**	**33**
5. Kategoria zagrożenia: Nieumiejętne posługiwanie się systemem przez administratora					
1. Brak właściwych szkoleń administratorów w zakresie użycia systemu	**2**	**3**	**2**	**3**	**16**
2. Brak kontroli jakości danych wprowadzanych do systemu	**1**	**2**	**3**	**3**	**8**
3. Odzyskiwanie informacji z nośników wycofanych z użycia	**3**	**4**	**0**	**4**	**24**
4. Podatność użytkowników na oddziaływanie metod inżynierii społecznej w celu uzyskania informacji lub wprowadzenia kodu złośliwego	**3**	**3**	**4**	**3**	**30**
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**	**5**	**4**	**5**	**14**
9. Rutyna i/lub nadmiar obowiązków administratora	**2**	**4**	**1**	**2**	**14**
10. Błędy i pomyłki w zarządzaniu systemem.	**3**	**4**	**2**	**3**	**27**
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	**2**	**3**	**4**	**3**	**20**
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)	**3**	**2**	**2**	**2**	**18**
6. Brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja 7. oprogramowania IPS/IDS i jego sond	**3**	**3**	**2**	**2**	**21**
7. Ujawnienie hasła administratora	**3**	**5**	**3**	**4**	**36**
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**	**2**	**1**	**4**	**7**
4. Podsłuch informacji w sieci wewnętrznej (LAN)	**2**	**1**	**0**	**3**	**8**
5. Pozyskanie informacji z nośników wycofanych z użycia	**2**	**1**	**1**	**3**	**10**
6. Nieuprawnione wykorzystanie/modyfikowanie urządzeń	**1**	**2**	**1**	**4**	**7**
7. Wykorzystanie podsłuchu programowego	**3**	**1**	**1**	**2**	**12**
8. Kategoria zagrożenia: Włamanie do systemu teleinformatycznego z sieci zewnętrznej WAN (przełamanie zabezpieczeń)					
1. Brak aktualizacji oprogramowania systemowego	**3**	**3**	**2**	**2**	**21**
2. Brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja zapór sieciowych (firewall)	**2**	**3**	**3**	**4**	**20**
3. Brak, niewłaściwe umiejscowienie w topologii sieci lub zła konfiguracja oprogramowania IPS/IDS i jego sond	**2**	**2**	**3**	**3**	**16**
4. Brak nadzoru nad ruchem sieci (QoS)	**2**	**3**	**3**	**2**	**16**

5. Brak monitorowania obciążenia serwerów	**1**	**2**	**2**	**0**	**3**
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	**1**	**2**	**3**	**1**	**6**
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**	**3**	**2**	**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**	**5**	**20**

5. Wnioski

Poziomy ryzyka:

- Ryzyko $R_p \leq 9.6$ - przyjmujemy je jako akceptowalne - zbyt małe i nieopłacalne, aby je wyeliminować (21 rodzajów z 63)

- Ryzyko $R_p \in (9.6, 38.4>$ - należy wprowadzić pewne zabezpieczenia, które mogłyby zniwelować zagrożenie występujące w tej kategorii (42 rodzajów z 63)

- Ryzyko $R_p > 38.4$ - w tym przypadku ryzyka, należy bezzwłocznie zareagować wdrążając wymagane zabezpieczenia. W przypadku braku możliwości, zgłosić zdarzenia do odpowiednich podmiotów (0 rodzajów z 63)

Działania:

- Przeprowadzanie okresowo audytów bezpieczeństwa - również związanych z daną tematyką ataku - w celu uniknięcia (zminimalizowania) zjawiska kolejnego ataku

- Powołanie oddziału lub rozdzielenie zadań pewnej grupa osób, która będzie miała za zadanie sprawdzanie najnowszych wersji oprogramowania/wdrażanie najnowszych wersji systemów

- Postawienie na rozwój w kierunku bezpieczeństwa systemów zarządzanymi przez administratorów (np. zwiększenie budżetu na szkolenia/samoedukację)

- Wymuszenie częstej zmiany haseł, w tym pamiętanie standardach długości i złożoności haseł (np. NIST-owych). Dot. wszystkich pracowników w danej firmie, oddziale

- Wdrożenie pewnego systemu bezpieczeństwa, który gromadził by logi oraz je analizował. W ten sposób zwiększamy szansę wykrycia wszelkich anomalii czy prób włamań do systemów