PREZYDENT MIASTA KRAKOWA

OR-03.0003.881.2024

Pan
Łukasz Gibała
Radny Miasta Krakowa

Odpowiadając na Pana interpelację w sprawie ataku hakerskiego na systemy informatyczne MPK SA w Krakowie, przekazaną przez Pana Jakuba Koska, Przewodniczącego Rady Miasta Krakowa 18 grudnia 2024 r., uprzejmie informuję.

Odpowiedzi na pytania zawarte w interpelacji były przedmiotem wystąpienia Prezesa Miejskiego Przedsiębiorstwa Komunikacyjne SA w Krakowie podczas sesji Rady Miasta Krakowa 18 grudnia 2024 r.

Ad 1.

Pierwsze problemy z systemami informatycznymi zostały zauważone 3 grudnia 2024 r. około godziny 7:00. Były to problemy z dostępem do zasobów informatycznych Spółki.

Ad 2 i 4 .

Według danych posiadanych przez Spółkę prawdopodobnie był to atak ransomware – MPK nie posiada wszystkich informacji o wektorze ataku.

Ad 3.

Narażone na ryzyko zostały dane składowane na serwerach Spółki, w tym dane pasażerów, pracowników, kontrahentów. Aktualnie Spółka nie posiada żadnego potwierdzenia, aby jakiekolwiek dane zostały wykradzione.

Ad 5.

Obecnie trwa śledztwo w tej sprawie.

Ad 6.

Systemy bezpieczeństwa nie wykryły próby włamania zanim doszło do naruszenia.

Ad 7 i 9.

Po zdiagnozowaniu sytuacji rozpoczęto informowanie następujących instytucji - 3 grudnia 2024 r. zdarzenie zgłoszono do Centrum Obsługi Informatycznej Urzędu Miasta Krakowa, Computer Emergency Response Team (CERT), Policji, Agencji Bezpieczeństwa Wewnętrznego, Naukowej i Akademickiej Sieci Komputerowej (NASK),

Dowody zostały zabezpieczone, a Spółka wykonywała polecenia (NASK), Policji i Centrum Obsługi Informatycznej UMK w zakresie bezpieczeństwa i dostarczania materiałów dowodowych. W dniu 4 grudnia 2024 r. nastąpiło zgłoszenie incydentu do Urzędu Ochrony Danych Osobowych.

Również Zarząd Transportu Publicznego w Krakowie podjął odpowiednie działania zabezpieczające, tj.:

- zablokowano wszystkie kanały komunikacji elektronicznej ZTP - MPK (na poziomie urządzeń sieciowych i usług chmurowych);
- podjęto intensywną komunikację telefoniczną i e-mailową z podwykonawcami i instytucjami współpracującymi z ZTP w zakresie systemów TTSS celem zablokowania dostępów i połączeń sieciowych z MPK;
- przeprowadzono pełne skanowanie urządzeń użytkowników i sieciowych w ZTP pod kątem ew. nieprawidłowości;
- zresetowano hasła wszystkich użytkowników usług ZTP;
- przeprowadzono weryfikację poprawności i odtwarzalności danych z backupów systemów informatycznych ZTP itp.;
- poinformowano pracowników ZTP o zaistniałej sytuacji, wynikających z niej zagrożeniach oraz wydano zalecenia dotyczące postępowania z korespondencją elektroniczną oraz fizycznymi nośnikami danych podpinanymi do komputerów w ZTP;
- opublikowano na stronie internetowej ZTP informacje o naruszeniu ochrony danych;
- skierowano korespondencję do MPK mającą na celu uzyskanie pełnych i szczegółowych informacji dotyczących wektora ataku oraz innych niezbędnych do obsługi incydentu;
- skierowano zawiadomienie do Prezesa Urzędu Ochrony Danych Osobowych;
- zażądano i uzyskano od podwykonawców ZTP informacje o stanie zabezpieczeń i komunikacji systemów z infrastrukturą i systemami MPK;
- przeprowadzono analizę logów systemów informatycznych ZTP;
- przeprowadzono nadzwyczajną weryfikację aktualności systemów informatycznych ZTP w zakresie instalacji patchy bezpieczeństwa;
- zainicjowano spotkanie u Prezydenta Miasta Krakowa celem ustalenia stanu faktycznego w aspekcie ataku hackerskiego oraz możliwych do zaimplementowania działań interwencyjnych;
- uruchomiono awaryjną stronę internetową z rozkładami jazdy KMK;
- zwołano i przeprowadzono regularne spotkania ISIRT ZTP;
- nastąpiło dodatkowe otwarcie 14 grudnia 2024 r. (sobota) stacjonarnych Punktów Obsługi Pasażerów w godzinach 08:00- 13:00;
- po potwierdzeniu bezpieczeństwa systemów po stronie MPK, od 10 grudnia 2024 r. rozpoczęto sukcesywne przywracanie działania systemów sprzedażowych i transportowych.

Ad 8.

MPK SA w Krakowie posiada procedury reagowania na incydenty bezpieczeństwa. Również Zarząd Transportu Publicznego w Krakowie posiada wdrożoną Politykę Bezpieczeństwa Informacji, w której uwzględniono procedury reagowania na incydenty bezpieczeństwa. Procedury były wdrożone przed atakiem.

Ad 10.

W dniu 3 grudnia 2024 r. zgłoszenie do Centrum Obsługi Informatycznej Urzędu Miasta Krakowa. Centrum Obsługi Informatycznej zabezpieczyło systemy Urzędu Miasta Krakowa poprzez wyłączenie usług integracyjnych z systemami MPK, wyłączenie tuneli VPN oraz zablokowanie ruchu przychodzącego z adresów sieciowych MPK oraz podmiotów powiązanych. Dotychczas Centrum Obsługi Informatycznej nie zaobserwowało żadnych istotnych skutków ataku na systemy MPK SA w Systemie Informatycznym UMK. Natomiast 4 grudnia 2024 r. około godz. 9.10 zgłoszono incydent do Inspektora Ochrony Danych Osobowych Zarządu Transportu Publicznego w Krakowie. W dniu 4 grudnia br. poinformowano również o ataku na serwery Zarząd Dróg Miasta Krakowa.

Ad 11.

Podjęto dodatkowe działania zabezpieczające systemy. Informacje szczegółowe tego typu stanowią tajemnicę przedsiębiorstwa.

Ad 12.

Spółka przeprowadziła audyty bezpieczeństwa wybranych systemów. Informacje szczegółowe tego typu stanowią tajemnicę przedsiębiorstwa.

Ad 13.

W MPK pracownicy byli szkoleni w zakresie cyberbezpieczeństwa oraz zarządzania usługami. Informacje szczegółowe tego typu stanowią tajemnicę przedsiębiorstwa. Natomiast w ZTP w 2024 r. przeprowadzono szkolenia z zakresie:

- ochrony danych osobowych i prywatności;
- stosowania środków zapewniających bezpieczeństwo informacji;
- naruszeń zasad bezpieczeństwa informacji i odpowiedzialność;
- wdrożonej Polityki Bezpieczeństwa Informacji i procedur z niej wynikających.

Ad 14.

Zdaniem Spółki dane były odpowiednio zabezpieczone.

Ad 15.

Spółka posiada stosowne kopie zapasowe. Informacje szczegółowe tego typu stanowią tajemnicę przedsiębiorstwa.

Ad 16.

Trwa śledztwo Policji oraz CERT. Na potrzeby śledztwa zostały zabezpieczane materiały. Spółka dodatkowo zleciła dodatkowe analizy firmie zewnętrznej. Informacje szczegółowe tego typu są objęte tajemnicą postępowania przygotowawczego - art. 241 ustawy z dnia 6 czerwca 1997 r. *Kodeks Karny* (Dz. U. z 2024 r. poz. 17 ze zm.).

.

Ad 17.

Informacje szczegółowe tego typ stanowią tajemnicę przedsiębiorstwa.

Ad 18.

Wynagrodzenia zostały w pełni wypłacone pracownikom Spółki i kontrahentom.

Ad 19.

Spółka poniesie koszty nadgodzin pracowników. Aktualnie nie są znane inne koszty dodatkowe.

z up. PREZYDENTA MIASTA

Signed by / Podpisano przez:
Antoni Jan Fryczek
Gmina Miejska Kraków - Urząd Miasta Krakowa
Date / Data: 2025-01-02 11:55

Antoni Fryczek
Sekretarz Miasta Krakowa

Otrzymują:

1. Adresat
2. Centrum Obsługi Informatycznej
3. Zarząd Transportu Publicznego w Krakowie
4. Miejskie Przedsiębiorstwo Komunikacyjne SA w Krakowie
5. Wydział Miejskiego Inżyniera Ruchu
6. Wydział Bezpieczeństwa i Zarządzania Kryzysowego
7. Wydział Organizacji i Nadzoru (OR-13)
8. Biuletyn Informacji Publicznej
9. aa