Treść odpowiedzi na interpelację radnego Stefana Traczyka w sprawie ataków hakerskich na system informatyczny Urzędu Marszałkowskiego Województwa Mazowieckiego

odpowiadając na interpelację z 20 kwietnia 2021 r. w sprawie ataków hakerskich na system informatyczny Urzędu Marszałkowskiego Województwa Mazowieckiego w Warszawie, poniżej przekazuję odpowiedzi na poruszane przez Pana kwestie.

1. **Czy Urząd Marszałkowski Województwa Mazowieckiego w Warszawie zanotował w roku 2020 i 2021 przypadki prób ataków hakerskich i czy podjęto jakieś działania zapobiegawcze?**

W 2020 roku zanotowano przypadki prób ataków hakerskich polegających na rozsyłaniu na konta mailowe pracowników Urzędu e-maili, mających charakter phishingu (Atak phishingowy to atak, w ramach którego haker próbuje oszukać jak największą liczbę użytkowników używając metod socjotechnicznych, aby zdobyć ich loginy, hasła, numery kart kredytowych lub wrażliwe dane firmowe albo aby zainfekować komputery użytkowników wirusami). Pracownicy Urzędu zgłosili wówczas 19 prób ataków phischingowych. Natomiast w 2021 roku takich prób było 25.

We wskazanych latach nie odnotowano żadnego skutecznego ataku phishingowego. Większość tego typu wiadomości jest filtrowana przez zabezpieczenia serwera poczty e-mail. Nie odnotowano także żadnego skutecznego ataku phishingowego zawierającego złośliwy załącznik. Przypadki, które docierają do kont e-mailowych pracowników są zgłaszane zespołowi CSIRT NASK zgodnie z ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Pracownicy Urzędu są ostrzegani o wykrytych kampaniach phishingowych stosownymi komunikatami. Adresy mailowe z których docierają wiadomości phishingowe są blokowane, a w przypadku gdy zawierają odnośniki do złośliwych domen, CSIRT NASK blokuje taką domenę.

Oprócz wdrażanych własnych rozwiązań technicznych zmniejszających ryzyko skutecznego ataku hakerskiego Urząd Marszałkowski Województwa Mazowieckiego w Warszawie przystąpił do projektu Ministerstwa Cyfryzacji i CERT Polska *„Partnerstwo dla cyberbezpieczeństwa”* oraz do pilotażu usługi CERT Polska *„Poszukiwania publicznie dostępnych danych uwierzytelniających”.* Usługa ta ma na celu monitoring wycieku danych uwierzytelniających oraz osobowych ze wskazanych przez Urząd domen.

Ponadto, pracownicy Urzędu są szkoleni z zakresu zagadnień związanych z tzw. cyberhigieną. W ramach strony intranetowej Urzędu prowadzona jest zakładka Cyberbezpieczeństwo zawierająca m.in. cotygodniowe zaobserwowane przez CERT Polska zagrożenia cberbezpieczeństwa z danego okresu okresu, komunikaty oraz poradniki z zakresu cberbezpieczeństwa.

Jednocześnie, Urząd Marszałkowski Województwa Mazowieckiego w Warszawie wykorzystuje następujące rozwiązania techniczne, służące zapewnieniu ochrony przez cyberatakami:

a) system antywirusowy, antyspywarowy i antyspamowy, zapewniający również: blokowanie programów typu exploit, ochronę przed botnetami, ochronę przed ransomware, ochronę przed lukami w protokołach sieciowych;
b) system ochrony styku sieci Urzędu z siecią Internetową klasy Enterprise UTM;
c) system rozszerzonego wykrywania i reagowania na zagrożenia;
d) sprzętowe i programowe zapory sieciowe (firewalle);
e) system DLP (Data Lost/Leak Protection);
f) sprzętowy Reverse Proxy.

2. Kiedy ostatecznie planuje się modernizację systemu obsługującego zdalne prace Sejmiku Województwa Mazowieckiego, w ten sposób aby obniżyć jego bieżące niedociągnięcia?

System eSESJA obsługujący zdalne prace Sejmiku Województwa Mazowieckiego składa się z dwóch części:

a) aplikacji eSesja, która zawiera repozytorium informacji oraz dokumentów, pozwala zarządzać organizacją sesji, udostępniać materiały, przeprowadzać głosowania. Część ta działa prawidłowo, bez większych usterek powodujących dokuczliwość dla uczestników sesji. Usterki te są usuwane na bieżąco, skutecznie przez dostawcę systemu.

b) modułu komunikacyjnego wideokonferencji on-line, którego funkcjonowanie stwarza problemy natury technicznej. Dotyczą one m.in. losowo braku obrazu (mimo, że kamera uczestnika jest włączona), losowo nieudane wczytanie prezentacji, losowo zerwanie połączenia transmisji. Z uwagi, że są to zdarzenia o charakterze losowym, analiza przypadków nie prowadzi do jednoznacznej identyfikacji przyczyn.

W lutym 2021 roku została podjęta próba wymiany modułu komunikacyjnego, która zakończyła się niepowodzeniem (proponowana zmiana w warunkach rzeczywistych powodowała więcej problemów, niż przed wymianą).Obecnie zaprojektowano nowe działania w kierunku wyeliminowania problemów. Są to:

- dostawca systemu uruchomi na potrzeby sesji Sejmiku Województwa Mazowieckiego odrębny, dedykowany serwer komunikacyjny. Dedykowany serwer zapewni większą kontrolę nad wydajnością i sprawnością wideokonferencji. W przypadku dalszych nieprawidłowości umożliwi pewniejszą i pełniejszą identyfikację problemów;

- na czas sesji dostawca systemu wskaże dedykowane osoby do udzielania wsparcia technicznego oraz rozwiązywania bieżących problemów, wymagających interwencji dostawcy;

- przed sesją zostaną uruchomione testy weryfikacyjne dotyczące zgodności wymagań systemu z rzeczywistym środowiskiem teleinformatycznym sesji Sejmiku Województwa Mazowieckiego.

Działania te będą wykonane w terminie przed planowaną w maju 2021 roku sesją Sejmiku.