Ataki hakerskie na bazy danych w starostwach w Chełmnie i Oświęcimiu

Realne konsekwencje cyberparaliżu

W ostatnich tygodniach geodeci z dwóch powiatów oddalonych od siebie o ponad 300 km doświadczali tych samych trudności. Nie mogli – lub nadal nie mogą – zgłosić nowej pracy w PODGiK-u czy pobrać materiałów zasobu i to zarówno elektronicznie, jak i na miejscu w urzędzie.

Damian Czekaj

Jeszcze przed usunięciem awarii o problemach w chełmińskim PODGiK-u rozmawialiśmy z lokalnym wykonawcą. – Byliśmy scyfryzowani i wszystko do tej pory działało pięknie – podkreślał. Zapytany o zlecenia, nasz rozmówca przyznał, że jest w sytuacji o tyle komfortowej, że obecnie realizuje duże prace, więc w najbliższym czasie będzie miał co robić. – Najgorzej mają ci geodeci, którzy robią „drobiazgi". Im praca szybciutko się skończy – zauważył.

Powiat chełmiński

O kłopotach PODGiK-u w Chełmnie na początku października poinformował nas jeden z czytelników GEODETY. Na stronie internetowej starostwa próżno było szukać informacji o utrudnieniach w obsłudze geodetów, dlatego skontaktowaliśmy się bezpośrednio z geodetą powiatowym Zbigniewem Bernackim, naczelnikiem Wydziału Geodezji, Kartografii i Gospodarki Nieruchomościami. – Na początku września dokonano włamania, zhakowano nasz serwer i zaszyfrowano dane – wyjaśnił GEODECIE. Chełmińska geodezja jest w pełni scyfryzowana, dlatego „padła" zarówno obsługa elektroniczna, jak i na miejscu w urzędzie. Geodeta powiatowy podkreślił, że o sprawie niezwłocznie poinformowane zostały odpowiednie służby – Komenda Powiatowa Policji w Chełmnie prowadzi postępowanie. Z kolei geodeci otrzymali maile zawiadamiające o utrudnieniach.

Przedmiotem ataku był tylko serwer bazy danych geodezyjnych, tym samym utrudnienia objęły jedynie komórki organizacyjne korzystające z PZGiK. – Posiadamy kopie zapasowe na dyskach serwera, dyskach zewnętrznych oraz

Praca zdalna sprzyja hakerom

Rozmawiamy z ARKADIUSZEM SIERADZKIM – właścicielem firmy Magnes Danych specjalizującej się m.in. w odszyfrowywaniu plików zablokowanych przez wirusy

DAMIAN CZEKAJ: Czy odszyfrowanie baz w Starostwie w Chełmnie nazwałby pan typowym zleceniem?

ARKADIUSZ SIERADZKI: Zdecydowanie nie. Mieliśmy tam do czynienia z bardzo skomplikowanym przypadkiem szyfrowania. Ponadto sprawa dotyczyła ogromnej ilości danych. Sama baza to setki gigabajtów, a w kilku kilobajtach mogą znajdować się nawet setki wierszy kodu. Dlatego nasza praca trwała blisko dwa i pół tygodnia.

Miesiąc później zaatakowane zostały bazy w Starostwie w Oświęcimiu. Do tej pory nie słyszeliśmy o takich sytuacjach. Przynajmniej nie w geodezji.

Na pewno wpływ na to ma pandemia koronawirusa. Wielu ludzi pracuje z domu i łączy się z serwerami za pomocą usług sieciowych. A hakerzy z reguły włamują się właśnie przez RDP, który umożliwia pracę zdalną [chodzi o protokół pulpitu zdalnego opracowany przez Microsoft – red.]. W biurze czy w urzędzie pracownik ma sieć udostępnianą lokalnie. Teraz wszystko jest uzewnętrzniane, więc ryzyko włamania rośnie.

Jak wygląda taki atak?

Zazwyczaj automatyczne boty skanują cały internet, szukając wypuszczonych na zewnątrz RDP. Po wytypowaniu potencjalnej ofiary

dodatkowej macierzy dyskowej, jednak część z nich również uległa zaszyfrowaniu. Zależało nam na przywróceniu jak najbardziej aktualnej, produkcyjnej bazy danych na nowym, zakupionym po ataku serwerze. Zakup ten był konieczny, ponieważ zainfekowany serwer został odłączony od sieci i na razie nie będzie używany. Może stanowić dowód w sprawie – tłumaczył Zbigniew Bernacki.

W odszyfrowaniu danych pomagała firma Magnes Danych z Warszawy (rozmowa z właścicielem firmy poniżej). Wsparcie zapewniła też Geomatyka-Kraków, w której systemie Ewid 2007 prowadzona jest chełmińska baza i z którą powiat ma podpisaną umowę asysty technicznej i konserwacji systemu. Po całej operacji odzyskiwania danych pracownicy WGKiGN sprawdzili co setną wybraną losowo jednostkę rejestrową, rejestr prac geodezyjnych i zmiany wprowadzone na numerycznej mapie zasadniczej na podstawie operatów. Szukali nieprawidłowości – przesunięć, skrętów itp. Na szczęście, nie znaleźli w bazie żadnych błędów. Obsługa geodetów w urzędzie została przywrócona 8 października, a dzień później ponownie ruszył internetowy Portal Geodety.

Jak podkreślił geodeta powiatowy, po ataku zakupiono urządzenie UTM do filtrowania ruchu między siecią lokalną a internetem. Zmianie uległy też zasady wykonywania i przechowywania kopii zapasowych.

Powiat oświęcimski

Kilka dni po „odmrożeniu" chełmińskiej geodezji z podobnym problemem musiało się zmierzyć starostwo w Oświęcimiu. Po ataku hakerskim „wysiadło" tam zgłaszanie prac, udostępnianie materiałów czy przyjmowanie prac geodezyjnych do zasobu, a także składanie projektów do uzgodnień na naradach koordynacyjnych. „Jesteśmy drugim powiatem w Polsce w takiej sytuacji, nie umiemy więc nawet precyzyjnie ocenić, jak długo będziemy odzyskiwać dane. Sytuacja może w naszej ocenie trwać nawet 2-4 tygodnie. Jednocześnie informujemy, że podjęliśmy intensywne działania zmierzające do odzyskania danych. O uruchomieniu systemu zostaną Państwo niezwłocznie powiadomieni" – napisała do wykonawców geodezyjnych Wioletta Nowak, geodeta powiatowy.

W Oświęcimiu 13 października zaatakowane zostały nie tylko dane geodezyjne, ale także wydziału inwestycji. W związku z tym wystąpiły utrudnienia w bieżącej pracy aż trzech wydziałów: Geodezji, Kartografii i Gospodarki Nieruchomościami, a także Architektury i Budownictwa oraz Inwestycji, Rozwoju i Dróg. Zaraz po ujawnieniu ataku zostały o nim powiadomione: policja, CERT Polska (zespół powołany do reagowania na zdarzenia naruszające bezpieczeństwo w sieci internet) oraz UODO.

– Za usunięcie awarii i zabezpieczenie odpowiadają pracownicy Wydziału Informatyki, natomiast odzyskanie danych geodezyjnych zleciliśmy firmie zewnętrznej – wyjaśnił GEODECIE naczelnik WI Dariusz Czerwik. – Starostwo posiada kopie baz danych geodezyjnych. Niestety, one także zostały zaszyfrowane, dlatego nie udało się ich przywrócić zaraz po ataku. Nie dopuszczamy jednak takiej możliwości, że danych geodezyjnych nie uda się odzyskać. Pracujemy nad tym, aby przywrócić pełną funkcjonalność wydziałów – zapewnił Dariusz Czerwik. Uruchomienie systemów oraz obsługi klientów urzędu może potrwać nawet kilka tygodni.

To nie wina programu do PZGiK

Starostwo w Oświęcimiu podobnie jak w Chełmnie wykorzystuje rozwiązania Geomatyki-Kraków, dlatego poprosiliśmy

wkracza haker i zaczyna nasłuchiwać jej działania. Jeśli w czasie tego nasłuchu użytkownik poprawnie zaloguje się do systemu, haker może przechwycić fragment odpowiedzi od serwera. To pozwala mu już na założenie własnego konta z uprawnieniami administratora i infiltrację sieci.

Od razu przystępuje do szyfrowania danych?

Nie, bo przeważnie systemy zabezpieczające na to nie pozwalają. Może upłynąć nawet kilka tygodni, nim program wykonujący ransomware [wirus – red.] zacznie działać. Wcześniej hakerzy dokładnie poznają architekturę sieci, przygotowują specjalne skrypty, wyłączają zabezpieczenia i systemy backupowe, które automatycznie co jakiś czas wykonują kopie zabezpieczające baz danych. Dopiero później rozpoczyna się szyfrowanie, najczęściej w nocy, kiedy z serwera nie korzysta żaden użytkownik. Szyfrowane są wszystkie dane, nawet kopie bezpieczeństwa, jeżeli nośniki z nimi nie zostały odłączone od sieci.

Jak zatem zabezpieczyć się przed takim atakiem?

Podstawą jest systematyczne robienie kopii na zewnętrznych dyskach odłączanych od sieci natychmiast po nagraniu. Na pewno oprogramowanie Microsoftu [RDP – red.] nie jest idealne, są w nim dziury, które wykorzystują hakerzy. Może gdyby część została załatana… Ale nie oszukujmy się, hakerzy zawsze będą lepsi od programistów.

Pewnym rozwiązaniem jest też audyt sieci w biurze czy urzędzie. Biorę wtedy dwóch najlepszych hakerów w Polsce i każę im znaleźć słabe punkty w systemie informatycznym. Ale to są koszty rzędu kilkuset tysięcy złotych. Nie każdy może sobie na to pozwolić.

PODGiK-i w Chełmnie i Oświęcimiu korzystają z tego samego systemu do prowadzenia zasobu.

To może być przypadek. Hakerzy nasłuchują kogo się da, a o tym, kto jest ofiarą, dowiadują się dopiero wtedy, gdy już włamią się do sieci.

Czy już teraz można określić, kto odpowiada za atak w Chełmnie?

Ransomware, który zaatakował chełmińskie bazy, należy do grupy około 300 cyberprzestępców różnej narodowości, głównie ze wschodu. Takie wirusy można kupić w darknecie, grupy hakerskie handlują między sobą kodami źródłowymi.

Co się dzieje po odzyskaniu danych?

Pałeczkę przejmuje policja. W toku śledztwa muszą się dowiedzieć, w jaki sposób doszło do ataku. My tylko odzyskujemy dane.

Rozmawiał Damian Czekaj