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

tę firmę o komentarz. – Skieruję kilka słów ostrzeżenia do innych potencjalnych ofiar: proszę, nie spodziewajcie się, że zabezpieczenia części webowej oprogramowania do prowadzenia baz danych PZGiK zastąpią profesjonalne urządzenia sieciowe, jak UTM-y, routery i firewalle przeznaczone do zabezpieczania serwerów i sieci lokalnych – zaapelował dyrektor generalny Geomatyki-Kraków Jacek Łaguz.

Odnosząc się do sugestii (m.in. komentarzy na Geoforum.pl), że ataki umożliwiły błędy w rozwiązaniach Geomatyki-Kraków, Jacek Łaguz zaznaczył, że nie zostały złamane żadne zabezpieczenia oprogramowania do prowadzenia PZGiK, żadne dane nie wyciekły, a bazy nie zostały zablokowane, lecz zniszczone przez szyfrowanie. – Zatem obydwa incydenty nie mają nic wspólnego z zabezpieczeniami dostarczanego przez nas oprogramowania. Informacje, jakie udało nam się uzyskać, wskazują na to, że zostały złamane zabezpieczenia serwerów, na których znajdowały się bazy danych. Następnie zaszyfrowano wszystkie, a nie tylko geodezyjne, znajdujące się tam pliki – wyjaśnił.

Jacek Łaguz zapewnił, że oprogramowanie Geomatyki-Kraków jest projektowane, tworzone i rozwijane z uwzględnieniem standardów bezpieczeństwa, podlega też aktualizacjom, w tym zabezpieczeń – to standardowa procedura wsparcia technicznego. Jednocześnie przyznał, że analiza znanych okoliczności ataków nie wykazała konieczności dokonania modyfikacji zabezpieczeń.

– Obydwa incydenty to coś więcej niż tylko ataki hakerskie. To cyberterroryzm, którego znakiem rozpoznawczym jest żądanie okupu i niszczenie. Niestety, w przyszłości należy spodziewać się eskalacji tego zjawiska i zauważyć jego bezpośredni związek z pandemią COVID-19. Wynika to wprost ze wzrostu skali wykorzystania rozwiązań e-commerce (nie tylko e-usług publicznych) oraz komunikacji i pracy zdalnej. Dla systemów bezpieczeństwa, które zostały zbudowane w warunkach dominacji tradycyjnych form komunikacji, jest to sytuacja wymagająca nie tyle rygorystycznego egzekwowania ustalonych reguł, co dokonania przeglądu ich adekwatności do nowej sytuacji i, z dużym prawdopodobieństwem, zaktualizowania stosowanych zabezpieczeń: zarówno technicznych, jak i organizacyjnych – podkreślił dyrektor generalny Geomatyki-Kraków.

Nowe idzie

Na razie w sprawie ataków niewiele rzeczy wiemy „na pewno”. Sposoby działania hakerów w wywiadzie udzielonym GEODECIE przybliżył Arkadiusz Sieradzki, właściciel firmy Magnes Danych. Podobnie jak Jacek Łaguz powiązał on cyberataki z pandemią koronawirusa i częściej stosowaną pracą zdalną.

Rzecznik prasowy Komendy Powiatowej Policji w Chełmnie asp. szt. Tomasz Winiarski poinformował GEODETĘ, że w KPP pod nadzorem Prokuratury Rejonowej w Chełmnie prowadzone jest obecnie postępowanie w kierunku art. 268 § 1 kodeksu karnego. Paragraf ten mówi, że „kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2”. – Z uwagi na dobro postępowania wszelkie informacje w sprawie udzielone zostaną po jego zakończeniu – zaznaczył rzecznik.

Cyberatakami zainteresował się też główny geodeta kraju. – Podjęliśmy możliwe działania, aby podobnym sytuacjom zapobiegać w przyszłości – zapewnił Waldemar Izdebski. – Odbyliśmy odpowiednie spotkania informacyjne z pracownikami administracji oraz firmami dostarczającymi oprogramowanie do powiatów. Dodatkowo wysłaliśmy do wszystkich powiatów pisma informujące o atakach z prośbą o podjęcie działań zabezpieczających i wykazywanie czujności – dodał.

W całej tej sprawie nie można jednak zapomnieć o wykonawcach prac geodezyjnych. To ich i ich klientów najmocniej dotknęły cyberataki. W Chełmnie przez miesiąc nie mogli załatwić żadnej sprawy w PODGiK-u, a co za tym idzie – zakończyć prac czy rozpocząć nowych. Nie wiadomo dokładnie, ile może potrwać paraliż w Oświęcimiu. Jak wytłumaczyć klientowi miesięczne opóźnienie? To kolejny cios w trudnych czasach koronawirusa. Cyfryzacja danych jest nieunikniona i niesie za sobą wiele pozytywnych aspektów (o niektórych z nich piszemy w raporcie nt. stanu informatyzacji powiatów na s. 14). Jednak z nowymi technologiami wiążą się nowe zagrożenia, na które trzeba być przygotowanym i umieć właściwie odpowiedzieć.

Damian Czekaj

Komentarze do wiadomości dotyczących cyberataków opublikowanych na Geoforum.pl 8 i 16 października

~ostatnie pytanie to żart | 2020-10-08 08:16:51
Czyli nie było backupowania, skoro dane trzeba było odszyfrowywać? Czy system funkcjonujący w ośrodku przechodził testy bezpieczeństwa albo miał certyfikację?

~pesymista | 2020-10-08 08:49:11
No to dzięki przepisom, które nam zafundował na wniosek naszego GGK ustawodawca, dobrze przeprowadzony atak hakerski zatrzyma proces inwestycyjny w całym kraju i działalność urzędów w sprawach wymagających dokumentacji geodezyjnej. Przecież musi to być zgłoszone i zweryfikowane. Bo oczywiście przepisów na taką sytuację kryzysową nie ma.

~geoinfo | 2020-10-08 10:42:00
Pracownicy/firmy dzielą się na dwie grupy. Tych, co robią kopie zapasowe, i tych, co będą robić kopie zapasowe. Kopie oczywiście trzymamy na płycie CD/DVD/zewnętrznym HDD/pendrivie/komputerze odciętym od sieci. Inaczej to nie ma sensu.

~anonim | 2020-10-16 11:11:3
Praca zdalna otwiera wiele możliwości. Wystarczą dwie rzeczy: podłączenie pod zdalny pulpit w pracy oraz niewyłączenie i niewylogowanie komputera w domu. Do tego brak zabezpieczeń domowego komputera od antywirusów poprzez brak aktualizacji systemu Windows. To tak, jakbyśmy wyjechali na wakacje, zostawiając bramę i drzwi otwarte. Kwestia backupów to podstawa, inaczej trzeba zapłacić w USD, bo innej rady nie ma...

~Geo | 2020-10-16 11:24:57
To drugi atak na system Geomatyki, niech reszta powiatów zadba o ochronę systemu.

~Pl | 2020-10-17 08:25:22
Urząd, który ma działać zgodnie z ustawą, będzie przywracał serwery 4 tygodnie? Przecież to jest śmiech na sali. Mają mieć kopie i tyle. Jak mój prywatny serwer by padł, to nikt by się nie przejmował, że nie oddaję roboty w terminie, tylko dostałbym na pewno karę.

~JanuszA | 2020-10-21 14:52:21
Do ludzi nietechnicznych trochę faktów. System ewidencji jest na Windowsie, który jest dziurawy jak ser szwajcarski. Backupy są, bo takie są wymagania odgórne dla instytucji, regulowane przez prawo. Hakerzy są lepsi niż osoby kodujące tworzące zabezpieczenia, a atakowane sieci są analizowane przez tygodnie, zanim nastąpi procedura szyfrowania.

Wybór i skróty Redakcji