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