IN.0003.2.2021 Mosina, dnia 22 października 2021 r.

Data wpływu: 25.10.2021 r.
Nr sprawy: BR.0003.572.2021

PANI
MAŁGORZTA KAPTUR
PRZEWODNICZĄCA RADY MIEJSKIEJ
W MOSINIE

Dot.: zapytania nr BR.0003.572.2021 z dnia 4 października 2021 r.

Odpowiadając na interpelację Radnego Pana Łukasza Kasprowicza w sprawie przekazania informacji dot. awarii systemu komputerowego w Urzędzie Miejskim w Mosinie, wyjaśniam co następuje:

1. Awaria miała miejsce 16 września 2021 r. ok. godz. 20.30.
2. Awaria swoim zasięgiem objęła praktycznie cały system teleinformatyczny tut. Urzędu. Mimo stosowania wysokiej klasy zabezpieczeń (w tym m. in. urządzenia klasy UTM chroniącego punkt styku WAN/LAN oraz centralnie zarządzanego programu antywirusowego o rozszerzonym zakresie ochrony, a także wirtualnej segmentacji sieci) wyłączone z użytkowania zostały fizyczne serwery produkcyjne, działające na nich serwery wirtualne oraz stacje robocze. W zakresie szkód, należy zaznaczyć, że wszystkie systemy serwerowe, zostały odtworzone bez jakichkolwiek strat. Jedynym wyjątkiem są systemy dziedzinowe (podatki, księgowość, ewidencja ludności itp.), które zostały odtworzone z kopii zapasowych sporządzonych w godzinach okołopołudniowych w dniu 16.IX.2021 r., co oznacza, że ew. straty obejmowały maksymalnie ok. 3 h pracy. Realne straty dotyczą jedynie stacji roboczych, z których 13 zostało całkowicie zaszyfrowanych – oznacza to utratę plików zapisywanych przez ich użytkowników jedynie na dyskach lokalnych. Pozostałe stacje robocze nie zostały zaszyfrowane a pliki zapisywane na dyskach sieciowych zostały odtworzone bez jakichkolwiek strat.
3. Powodem awarii była infekcja oprogramowaniem typu ransomware z rodziny REvil/Sodinokibi.
4. Awarie i przestoje spowodowane infekcjami oprogramowaniem typu ransomware, są obecnie jednym z najpoważniejszych zagrożeń dla wszelkiego typu systemów teleinformatycznych, na całym świecie. Jest to proceder, za którym stoją zorganizowane grupy przestępcze, dla których jest to przede wszystkim źródło dochodu. Najczęstszym wektorem ataku w takich przypadkach jest kompromitacja połączeń RDP, e-mail phishing lub wykorzystywanie luk w oprogramowaniu. Ochrona przed tego typu atakami jest bardzo trudna, czego najlepszym potwierdzeniem jest rosnąca liczba infekcji dotykająca tysiące podmiotów na całym świecie. Z danych Check Point Research wynika, że średnio 1 na 61 organizacji na świecie została w jakiś sposób zainfekowana oprogramowaniem typu

ransomware. W Polsce, jeżeli chodzi o jednostki Samorządu Terytorialnego, tylko z tych medialnie nagłośnionych, tego typu ataki dotknęły m. in. Kościerzynę, Oświęcim, Turek i chociażby ostatnio Otwock, jednak należy pamiętać, że jest to jedynie "czubek góry lodowej", ponieważ bardzo wiele tego typu incydentów, często nie jest nawet zgłaszana. Należy pamiętać, że żaden z dostępnych obecnie na rynku programów antywirusowych i innych systemów zabezpieczeń nie gwarantuje 100% ochrony przed tego typu infekcjami, co oznacza, że podstawą przeciwdziałania jest backup danych, regularne inwestycje w nowy sprzęt i oprogramowanie, zapewnienie ciągłego rozwoju i odpowiednich warunków pracy służbom odpowiedzialnym za bezpieczeństwo teleinformatyczne, a także ciągła edukacja użytkowników.

W przypadku tut. Urzędu, w zakresie wdrożonych zmian w wyniku awarii, należy wymienić przede wszystkim podniesienie restrykcyjności policy stosowanych zarówno na UTM jak i w oprogramowaniu antywirusowym, planowane przeprowadzenie dodatkowych szkoleń z cyberbezpieczeństwa wśród pracowników oraz przystąpienie do wyboru nowego systemu backupowego, który pozwoli na zdecydowane zwiększenie częstotliwości sporządzania kopii zapasowych oraz obejmie swoim działaniem również stacje robocze. Na przyszły rok, zaplanowane są inwestycje, dofinansowane ze środków zewnętrznych, w infrastrukturę serwerową, w wyniku których m. in. zostanie stworzona druga serwerownia (na ul. Dworcowej 3), zostanie podniesiona wersja systemu serwerowego do poziomu Windows Server 2022 oraz zostanie wdrożony dodatkowy system tworzenia kopii zapasowych w oparciu o napęd taśmowy. Dodatkowo, Zespół Informatyków, uwzględnił we wniosku budżetowym na 2022 r. przydzielenie środków pozwalających na zakup serwera produkcyjnego do głównej serwerowni, który na razie pełniłby funkcję urządzenia awaryjnego (którego brak okazał się jednym z najpoważniejszych problemów), a docelowo, stałby się jednym z dwóch podstawowych serwerów klastra HA, który miałby zastąpić, obecnie stosowane rozwiązanie, dla którego nieuchronnie zbliża się termin EOL (End of Life). Należy też pamiętać, że wszelkie zmiany sprzętowe i programowe wymagają obsługi, zarówno tej wdrożeniowej, jak i również później tej eksploatacyjnej, a co za tym idzie wymaga to zaangażowania pracowników, którzy powinni dysponować odpowiednią wiedzą oraz czasem niezbędnym na realizację określonych zadań.

Z poważaniem

BURMISTRZ GMINY MOSINA
(-) Przemysław Mieloch

Otrzymują:
1. Adresat
2. Pan Łukasz Kasprowicz – Radny Rady Miejskiej w Mosinie
3. a/a

Sprawę prowadzi:

Bartosz Dmochowski
Kierownik Zespołu Informatyków
tel. 618-109-522
e-mail: admin@mosina.pl