Cyberbezpieczeństwo !!!

Podniesienie stopnia alarmowego CHARLIE-CRP do odwołania

Wynika z sytuacji za naszą wschodnią granicą, ale też serii cyberataków w Portugalii.

Jak informuje dr Piotr Łuczuk, ekspert ds. cyberbezpieczeństwa z Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie, ucierpiał sektor bankowy, został wręcz sparaliżowany. Portugalczycy mieli bardzo duży problem w dokonywaniu płatności elektronicznych czy z wypłacaniem pieniędzy z bankomatów. Łącząc te wszystkie fakty, jest realna groźba tego, że ktoś może wykorzystywać sytuację do siania jeszcze większego zamętu. Na tym właśnie polegają działania w cyberprzestrzeni. One są w dużej mierze rozproszone, przez co uderzają w różne aspekty życia społecznego.

Odnosząc się do stopni alarmowych CRP tłumaczy, że „dotyczą one zabezpieczenia strategicznej infrastruktury teleinformatycznej" i dodaje: „przez to należy rozumieć komunikację na szczeblu rządowym, możliwość zapewnienia niezakłóconych dostaw energetycznych czy pracy sektora bankowego".

Ostrzega, że „oprócz serii ataków ze wschodnim rodowodem, którym jesteśmy poddawani jako Polska co najmniej od roku 2016, o czym nieustannie informuje Stanisław Żaryn, do gry będą się włączać grupy hakerskie, które na tej sytuacji chcą skorzystać, chcą siać jeszcze większy zamęt".

Dr Łuczuk tłumaczy, że „tego typu ataki podyktowane są próbą zakłócenia komunikacji wszystkich szczebli, serwisów informacyjnych czy wręcz wywołania szumu informacyjnego".

- To też element wojny informacyjnej, którą de facto obserwujemy od dłuższego czasu. Mieliśmy przykłady tego, co regularnie punktował rzecznik ministra koordynatora służb specjalnych. Wskazywał przypadki złożonych kampanii dezinformacyjnych, wymierzonych przeciwko Polsce. W ich ramach wykorzystywano nawet publikacje w polskich, a także zagranicznych mediach. W miarę coraz większego rezonowania, powstawał szum informacyjny. Coraz trudniej było się zorientować, co jest prawdą, a co odpowiednio kolportowanym fake newsem.

- przypomina zdarzenia ostatnich miesięcy, ściśle powiązanych z sytuacją na polsko-białoruskiej granicy.

Dopytywany, czy wprowadzenie 3. stopnia alarmowego CRP wpłynie na życie społeczne, podkreśla: „w kontekście statystycznego Kowalskiego kluczowe będzie to, by stosować się do podstawowych zasad bezpieczeństwa w cyberprzestrzeni".

- W przypadku śledzenia bieżących informacji, weryfikujmy ich źródła. Sprawdzajmy ich wiarygodność. Z kolei używając bankowości elektronicznej, zwracajmy uwagę na urządzenia, z których korzystamy oraz okoliczności. Ze szczególną ostrożnością podchodźmy do nietypowych wiadomości i próśb - nawet od znajomych czy rodziny - które otrzymamy w najbliższym czasie, mogą za nimi stać próby wyłudzenia danych lub uzyskania dostępu do naszych urządzeń - ostrzega ekspert z Instytutu Staszica, autor pierwszej w Polsce książki na temat cyberwojny.
- Dziś mamy do czynienia z regularną cyberwojną. Trudno jest jednak wskazać jednoznacznie wszystkich aktorów na tym polu bitwy. Większość tych działań toczy się ponad naszymi głowami, na przestrzeni serwerowni czy po prostu w cyberprzestrzeni. Jest to cicha i tania wojna, ale wywołująca realne konsekwencje - uczula, by nie bagatelizować powagi sytuacji i podaje przykład:

„Wyobraźmy sobie, że celem cyberataku jest sektor bankowości (jak we wspomnianym już przypadku z Portugalii) - nagle nie jesteśmy w stanie wypłacać pieniędzy, a nie jesteśmy też na to przygotowani. Nie mówię, że należy teraz szturmować bankomaty i masowo wypłacać środki, bo uzyskamy wówczas efekt odwrotny od zamierzonego. Natomiast dobrą praktyką jest to, co proponował jakiś czas temu prezes Narodowego Banku Polskiego prof. Adam Glapiński, żeby trzymać w domu kwotę, która pozwoli funkcjonować mniej więcej przez jakieś dwa tygodnie. Dla każdego będzie to oczywiście inna kwota, dostosowana do realnych potrzeb i poziomu życia, jednak warto zadbać o posiadanie takiej bezpiecznej poduszki finansowej o której warto pamiętać, niezależnie nawet od tego, co dzieje się za naszą wschodnią granicą”.

Chroń swoje dane. Nie daj się hakerom:

1. Sprawdzaj, jakich uprawnień żąda instalowana aplikacja.

2. Nie klikaj w linki oraz załączniki. Jeśli otrzymasz podejrzaną wiadomość od znajomego, poświęć chwilę na zweryfikowanie jej. Hakerzy często podszywają się pod znajomych.

3. Nie podawaj w rozmowie (zwłaszcza telefonicznej) poufnych danych.

4. Nie wchodź na stronę banku przez link. Wpisuj adres lub korzystaj z tzw. zaufanych zakładek. Stosuj podstawowe zasady bezpieczeństwa takie jak używanie złożonych i indywidualnych haseł dla każdej strony i odwiedzanie tylko zaufanych witryn, bez względu na to, za pomocą jakiego urządzenia się łączysz.

5. Uważaj na płatności w aplikacjach mobilnych. Używaj tylko oficjalnych aplikacji, instalowanych z pewnych źródeł.