**Cyberatak na ePUAP krótko po przedłużeniu stopni alarmowych. Co może to oznaczać dla firm?**

* **Premier przedłużył okres obowiązywania stopni alarmowych BRAVO i CHARLIE-CRP do końca sierpnia 2023 roku, a niedługo później hakerzy zaatakowali platformę ePUAP.**
* **To wyraźny sygnał, że poziom cyberzagrożeń nie spada. Spać spokojnie nie mogą też przedsiębiorcy.**
* **Sposobem na utrudnienie cyberataków lub zmniejszenie ich skutków jest ścisłe stosowanie się do procedur, szyfrowanie danych i regularne szkolenie pracowników.**

31 maja premier Mateusz Morawiecki przedłużył okres obowiązywania drugiego stopnia alarmowego (BRAVO) i trzeciego stopnia alarmowego CRP (CHARLIE–CRP) na terytorium Polski oraz drugiego stopnia alarmowego (BRAVO) wobec polskiej infrastruktury energetycznej, znajdującej się poza granicami państwa – podało Rządowe Centrum Bezpieczeństwa. Stopnie obowiązują do 31 sierpnia, do godz. 23:59. Niedługo później, 13 czerwca, minister cyfryzacji Janusz Cieszyński podał informację o ataku DDoS na platformę ePUAP, służącą do załatwiania spraw urzędowych. Cyberatak nie sparaliżował jej całkowicie, ale doprowadził do utrudnień w świadczeniu usług.

– *Ataki hakerskie na instytucje publiczne już od kilku lat przybierają na sile. Do tej pory miały one w zdecydowanej większości wyłącznie typowo przestępczy wymiar, czyli kradzież danych lub wyłudzenie okupu. Ostatnie z kolei są niewątpliwie związane z rosnącym napięciem politycznym na linii Ukraina-Rosja. Niestety, jak widać, polskie instytucje także są zagrożone, dlatego wciąż podejmowane są decyzje o przedłużaniu stopni alarmowych. Uważam, że także przedsiębiorcy nie mogą spać zupełnie spokojnie. Skala i częstotliwość ataków pokazują, że wszyscy musimy zachować czujność, także biznes i użytkownicy prywatni* – mówi Patrycja Tatara, ekspertka ds. cyberbezpieczeństwa w Sprint S.A.

**Warto się dozbroić i doszkolić**

Stopień CHARLIE-CRP zobowiązuje pracowników administracji IT do przeglądu zasobów w przypadku obrony i wdrożenia planów ciągłości po wystąpieniu ataku. Oprócz tego obowiązują ich także zadania z dwóch poprzednich stopni (ALFA i BRAVO-CRP), wśród których znajduje się m.in. monitoring systemów, procedur i zadań, zwiększona czujność i dyspozycyjność personelu, a także całodobowe dyżury administratorów systemów kluczowych. Warto także dodać, że w dalszej perspektywie wzmocnieniu cyberbezpieczeństwa w Polsce służyć będą przepisy, które są już implikowane do krajowego prawodawstwa z unijnej dyrektywy NIS 2. Wśród podmiotów, których będą one dotyczyć, znajdują się także duże organizacje komercyjne z rozmaitych obszarów biznesu. Jednak o wzmocnienie bezpieczeństwa IT powinny zadbać również mniejsze firmy.

– *Najbardziej zagrożone, w przypadku ataku na instytucje publiczne, są największe organizacje i firmy. Ale nie można zapominać, że coraz częściej hakerzy liczą na ilość, a nie jakość ofiar. Dlatego i sektor MŚP jest w obszarze ich zainteresowania. To, co przedsiębiorcy mogą zrobić, to zadbać przede wszystkim o infrastrukturę cybersecurity i procedury bezpieczeństwa. Nie wystarczą już rozwiązania takie jak szyfrowanie łączy czy stosowanie zewnętrznych firewalli. Aby móc skutecznie się bronić należy doposażać się w rozwiązania klasy SIEM, WAF czy też EDR. Często hakerzy rezygnują z ataku, jak w trakcie prób uzyskania dostępu do infrastruktury powstrzymują ich od tego silne zabezpieczenia. I jeszcze jedno – bardzo ważną kwestią są też cykliczne szkolenia personelu w zakresie cyberbezpieczeństwa. Hakerzy często „polują” na szeregowych pracowników, licząc na ich nierzadko niższy poziom wiedzy na temat cyberzagrożeń niż wśród zatrudnionych w działach IT. Świadomy zespół w organizacji to bardzo ważny element zabezpieczeń IT w firmie* – dodaje Patrycja Tatara ze Sprint S.A.

**Stopnie alarmowe i niedawne incydenty**

Stopień BRAVO dotyczy zagrożenia terroryzmem. To drugi w czterostopniowej skali, stopień alarmowy. Wprowadza się go, jeśli istnieje zwiększone i przewidywalne zagrożenie zdarzeniem o charakterze terrorystycznym. MSWiA podkreśla, że stopień ma charakter prewencyjny i ma związek z aktualną sytuacją geopolityczną w regionie, czyli ataki hybrydowe prowadzone przez Rosję i Białoruś, wymierzone także w Polskę i inne kraje UE. Z kolei CHARLIE-CRP dotyczy cyberzagrożeń. Trzeci z czterostopniowej skali oznacza wysoki poziom zagrożenia w cyberprzestrzeni. Stopień alarmowy CHARLIE-CRP zobowiązuje instytucje publiczne do zachowania szczególnej czujności oraz intensywniejszego niż dotychczas monitorowania bezpieczeństwa systemów IT. Po raz pierwszy został wprowadzony 21 lutego 2022 roku i był już przedłużany. Przez ten czas odnotowano przynajmniej kilka incydentów – ich ofiarami były instytucje państwowe. Wśród nich warto wymienić ataki DDoS na serwery Senatu RP (27 października 2022 roku), ransomware na Centrum Zdrowia Matki Polki w Łodzi (3 listopada 2022 r.) oraz DDoS na Platformę eZamówienia (7 listopada 2022 roku). Z kolei w 2023 roku, na początku lutego, doszło do ataku credential stuffing na Profil Zaufany, a teraz hakerzy znów zaatakowali i tym razem ofiarą padł ePUAP. W tym roku podobne incydenty odnotowały także firmy, o czym informowano również w kontekście ataków na instytucje publiczne. Szczęśliwie, każde z tych zdarzeń nie wywołało poważniejszych skutków poza czasowym paraliżem, choć zagrożenie zazwyczaj było wysokie.

Źródło: Sprint S.A.