KMP BIAŁYSTOK

http://bialystok.policja.gov.pl/po2/aktualnosci/55300,Dostales-e-mail-od-szefa-Nie-rob-przelewu.html
2020-09-22, 23:23

DOSTAŁEŚ E- MAIL OD SZEFA? NIE RÓB PRZELEWU!

W ostatnim czasie do białostockich policjantów wpłynęła informacja dotycząca próby oszustwa polegającego na podszywaniu się przestępcy pod przełożonego z poleceniem przelania określonej kwoty na wskazane w wiadomości e-mail konto bankowe. Tym razem, dzięki czujności pracownika odpowiedzialnego za płatności, oszustom nie udało się wyłudzić blisko 30 tyś euro.

W miniona środę białostoccy policjanci zostali powiadomieni o usiłowaniu oszustwa, do którego doszło w jednym z białostockich szpitali. Oszustwo to polegało na tym, że przestępcy, podszywając się pod dyrektora tej placówki medycznej, wysłali do działu księgowego wiadomość e-mai z poleceniem wykonania przelewu kwoty blisko 30 tys. euro na wskazane konto bankowe. Na szczęście pracownik, który odebrał maila wykazał się czujnością i za nim wykonał przelew, sprawdził prawdziwość przesłanego polecenia. Szybko okazało się, że wiadomość nie została wysłana przez dyrektora, a oszustów.

Pamiętajmy!

Cyberprzestępcy do przeprowadzenia ataku przygotowują się bardzo rzetelnie. Najpierw przeprowadzają rekonesans - na stronach internetowych poszukują informacji na temat lokalizacji firmy, osób zajmujących kierownicze stanowiska, jak również informacji o jej kontrahentach. Chcą wiedzieć wszystko. Następnym krokiem są serwisy społecznościowe zrzeszające pracowników. Za ich pośrednictwem próbują zebrać jak najwięcej informacji o osobach zatrudnionych w firmie - to na nich skupia się największa uwaga cyberkryminalistów. W zależności od ich intencji, wybierają konkretnych pracowników, np., jeśli ich celem są pieniądze, swoją uwagę kierują na dział płatności. Jeśli zaś chcą zebrać informacje o pracownikach, atakują dział kadr. Z kolei, gdy chcą przechwycić bazy danych, wówczas będą namierzać segment IT. Jeśli cel i ofiara są już zidentyfikowane, przystępują do przeprowadzenia ataku. Najczęstszą techniką jest "spear phishing". Polega on na wysłaniu maili nie do dużej grupy osób, a wąskiego, doprecyzowanego zespołu (w odróżnieniu do "phishingu", który ma zasięg masowy).

Mail od szefa- problem polega na tym, że maile wyglądają dość realistycznie i są trudne do wykrycia. Sprawiają wrażenie, że pochodzą od kogoś, kogo się dobrze zna, z kim się współpracuje - często szefa. Przestępcy dbają też o szczegóły. Redagują maile, używając żargonu pracowniczego, zamieszczają logo firmy czy nawet oficjalny podpis osoby z zarządu. W dodatku, wiadomości są formułowane tak, by tworzyć uczucie pośpiechu, sugerować, by zadanie wykonano natychmiastowo i - czasami - nawet dyskretnie. Cyberprzestępca chce, by ofiara popełniła błąd jak najszybciej: zrobiła przelew, przekazała poufne informacje, przesłała ważny dokument. Co ważne, nie każda taka operacja odbywa się przy użyciu maila. Innym sposobem jest rozmowa telefoniczna. Przestępca może podszywać się np. pod prawnika. Telefon poprzedzony jest zazwyczaj e-mailem, w którym przestępca podając się za szefa uprzedza, że pracownik może się spodziewać takiego połączenia.

Apelujemy do pracowników odpowiedzialnych za transfery finansowe w instytucjach i firmach o czujność. Konkretny adres mailowy nie stanowi potwierdzenia, że wiadomość przyszła faktycznie od naszego przełożonego. Jeśli wydane polecenie wzbudza wątpliwości pracownika, powinien on jak najszybciej skonsultować się z szefostwem.

Ocena: 0/5 (0)

Tweetnij