baramundi

CHECKLISTY BARAMUNDI zapewniają zwięzłe i szczegółowe wskazówki ekspertów odnoszące się do częstych pytań i problemów. Więcej z nich można znaleźć na stronie www.baramundi.com/checklisty.

Jak rozpoznać phishing w 5 krokach?

Słowo phishing łączy wyrażenie Password Harvesting, czyli „wyłudzanie haseł” oraz słowo fishing, czyli „łowienie”. Obejmuje ataki za pośrednictwem wiadomości SMS, głosowych lub e-mail. Wyglądają, jakby pochodziły od zaufanej osoby lub instytucji. Ofiary ataków są proszone o podanie informacji, takich jak dane logowania czy numery kont, a nawet instruowane do wykonania przelewu bankowego. Po czym rozpoznać phishing?

Adres nadawcy

Sprawdź, czy adres nadawcy odpowiada znanemu i zweryfikowanemu kontaktowi. Błędy ortograficzne lub gramatyczne powinny być ostrzeżeniem.

Nazwa domeny

Należy również zwrócić uwagę na domenę, czyli nazwę za @. W tym przypadku literówki lub podobnie brzmiące słowa są popularną sztuczką, mającą na celu oszukanie nieostrożnych.

Spoofing (podszywanie się)

Przy niewielkich nakładach technicznych przestępcy imitują istniejące adresy e-mail. Dlatego nawet adresy, które wydają się poprawne, nie zawsze mogą być wiarygodne. W tym przypadku pomoże jedynie zwrócenie uwagi na treść wiadomości i szczegóły, takie jak np. pole „Reply-To” w nagłówku e-maila.

Niebezpieczne linki i załączniki

Często phishing skłania ofiary do pobrania złośliwego oprogramowania za pośrednictwem linków lub załączników. Dlatego przed kliknięciem w link należy zawsze sprawdzić adres URL. Aby to zrobić, przytrzymaj kursor myszy nad linkiem przez kilka sekund. Nie otwieraj załączników, chyba że o nie prosiłeś lub ich oczekiwałeś i masz 100% pewności, że są bezpieczne.

Weryfikacja

Phishing wykorzystuje zaufanie ofiar. Lepiej być nad wyraz ostrożnym i użyć osobnego, sprawdzonego przez siebie kanału kontaktu z nadawcą wiadomości. W tym przypadku można użyć na przykład numeru telefonu z oficjalnej strony internetowej.

W pigułce: Phishing jest poważnym zagrożeniem. Dlatego wszyscy pracownicy powinni być regularnie szkoleni z zakresu nowych metod cyberprzestępców. Kluczową rolę w zabezpieczaniu systemów odgrywa również pakiet baramundi Management Suite. Umożliwia on szybką i skuteczną dystrybucję regularnych aktualizacji i poprawek bezpieczeństwa, które eliminują luki w zabezpieczeniach.