dr inż. Łukasz Strzelecki
Milstar

„Fałszowanie danych nadawcy w poczcie elektronicznej (z ang. e-mail spoofing) – istota zagrożenia, konsekwencje i sposoby przeciwdziałania”

Wiele ataków cybernetycznych (w fazie początkowej), w szczególności względem systemów dobrze zabezpieczonych, czy wręcz odizolowanych od sieci publicznych wymaga pewnych aktywności ze strony ich użytkowników. Dopiero wykonanie sprowokowanego działania, np. otworzenie strony ukrytej pod adresem URL umieszczonym w wiadomości poczty elektronicznej (tzw. mail-u) lub wykonanie innej akcji, o którą poproszono w treści wiadomości, daje agresorom przyczółek umożliwiający wykonanie właściwego ataku, w tym typu APT (ang. Advanced Persistent Theats), którego skutkiem może być między innymi fraud ubezpieczeniowy. Z tego powodu powodzenie ataku często zależy od poziomu wiarygodności informacji przekazywanej w sfałszowanej wiadomości pocztowej, a na to duży wpływ ma to, kto zdaniem odbiorcy wiadomości jest jej nadawcą. Inaczej podchodzi się do informacji pozyskanej z nieznanego źródła, a inaczej od osoby zaufanej, czy będącej np. przełożonym w pracy. Dlatego przy inicjowaniu (nawet złożonych) ataków w pierwszej ich fazie często wykorzystywany jest tzw. e-mail spoofing, który polega na fałszowaniu danych na temat nadawcy wiadomości. Wartym podkreślenia jest to, że istnieją metody przeprowadzania tego nadużycia, które nie naruszają założeń obsługi protokołu SMTP (ang. Simple Mail Transfer Protocol) określonych w dokumencie normatywnym RFC 5321 i pokrewnych, a więc w tym zakresie są one uznane za działania dozwolone. Z tego też względu większość systemów poczty elektronicznej, a nawet systemów chroniących je przed różnego typu nadużyciami np. typu SPAM-em, nie jest stanie wykryć tego typu nadużycia. W prezentacji zostanie przedstawiona istota podatności protokołu SMTP na e-mail spoofing oraz sposoby zabezpieczania się przed tego typu zagrożeniami.