aut. Tomasz Fastyn 05.08.2016

BLACK HAT USA – NAJWIĘKSZA KONFERENCJA EKSPERTÓW CYBERBEZPIECZEŃSTWA

W związku z zakończoną już konferencją Black Hat USA, która odbywała się na przełomie lipca i sierpnia w Las Vegas podsumowaliśmy kilka ciekawych prelekcji. Black Hat USA to największa konferencja dotycząca tematyki cyberbezpieczeństwa w sektorze publicznym oraz wojskowym. Podczas wystąpień poruszane były problemy z edukacją pracowników oraz niedofinansowania sektora cyberbezpieczeństwa w ostatnich latach.

Podczas prezentacji Scotta Keoseyana oraz Keitha Brogana z Deloitte Cyber Risk padły bardzo mocne słowa potępiające ostatnie 15 lat działań biznesu w kwestii cyberbezpieczeństwa. Według nich przez ten okres tematyka bezpieczeństwa była spychana zawsze na drugi plan, głównie jeżeli chodzi o finansowanie rozwiązań pozwalających na odpowiednie przygotowanie infrastruktury. Głównym źródłem problemów, oprócz nieodpowiedniego zaplecza finansowego, ma być według Brogana brak odpowiednich umiejętności w firmach. – Czasami programy nie działają poprawnie. Ale zazwyczaj są one po prostu źle używane – powiedział Brogan podczas prezentacji. Scott Keoseyan zapytany dlaczego mimo zwiększania nakładów na cyberbezpieczeństwo w firmach, które mają wynosić obecnie 75 mld dolarów rocznie, nadal jesteśmy świadkami włamań do systemów firmowych odparł – Zmieniamy swoje podejście do prowadzenia firm tak szybko, że powoduję to wzrost zagrożenia wynikającego z używania nowych rozwiązań. Chcemy aby mechanizmy cyberbezpieczeństwa były łatwiejsze w obsłudze, ale jednocześnie użytkownicy wymagają coraz więcej od technologii, która z każdym dniem jest coraz bardziej zawiła – odpowiedział Keoseyan.

Wśród ciekawy wystąpień także pojawiła sprawa oszustw telefonicznych, które nawet w Polsce występują nagminnie. Według danych policji oszustwa typu na „wnuczka” i „policjanta” pozwoliły na kradzież ponad 32 mln złotych w 2015 roku, czyli o 13 mln złotych więcej niż rok wcześniej. Rozwiązaniem tego problemu zajęła się dr Juditha Tabron z uniwersytetu Hofstra, podkreśla jednocześnie, że najsłabszym ogniwem bezpieczeństwa jest nadal człowiek. Dlatego jej zdaniem, ludzie powinni przy używać odpowiednich mechanizmów dla zabezpieczenia się przed działaniami przestępców, choćby w rozmowach telefonicznych. Tabron przy pomocy językoznawstwa śledczego opracowała punkty, które pokazują schemat działania przestępców dążących do wyłudzania pieniędzy oraz informacji w rozmowach telefonicznych.

1. Nienaturalne pauzy podczas rozmowy są stosowane celowo przez oszustów, tak aby ich rozmówca powiedział coś zapełniając ciszę

2. Niezbyt przyjazne przerywanie rozmówcy

3. Stosowanie przez przestępców takich pytań, aby naturalną odpowiedzią na nie było słowo „tak”

4. Kontrola tematu rozmowy

5. Unikanie odpowiedzi na konkretne pytania, przekierowywanie rozmowy na inne tematy, zadawanie pytań przez oszustów pytań niezwiązanych z aktualnie omawianą sprawą

6. Odpowiednie nakierowanie rozmówcy na problem. Oszuści nie tworzą historii, starają się raczej wciągnąć rozmówce w ciąg zdarzeń, tworzą pozory zdarzenia, które wymaga interakcji.

Sama dr Tabron podkreśla, że trudno jest wyczuć, że w narracji oszustów coś jest nie tak, głównie z powodu ich umiejętności przy przeprowadzanych rozmowach. Ale według niej, zwracanie uwagi właśnie na pytania, na które wydaję się, że można odpowiedzieć tylko w jeden sposób, pomaga uniknąć większości oszustw.

W podobnym tonie swoją prezentację przedstawił Arun Vishwanath, profesor na Stanowym Uniwersytecie Nowego Jorku w Buffalo, który powiedział wprost – Dobrym rozwiązaniem jest, że wszyscy używają wiadomości e-mail, jednocześnie złą sprawą jest, że wszyscy mają dostęp do poczty elektronicznej – powiedział na wstępie Vishwanath. Według niego genezą włamań do firm w przynajmniej 20 proc. są ludzkie błędy, które bezpośrednio spowodowały włamania do sieci informatycznych. Według niego istnieją trzy główne problemy, które powodują, bezpieczeństwo sieci firmowych, rządowych oraz organizacji pożytku publicznego jest narażone w dużej mierze na ataki hakerskie. – Pierwszym z nich jest kontrola pracowników nad takimi elementami cyberbezpieczeństwa jak zapory sieciowe. Powinniśmy ograniczyć użytkownikom możliwość dostępu do mechanizmów zabezpieczających infrastrukturę i jednocześnie ograniczyć ich uprawnienia administracyjne. Problem także występuję przy edukacji pracowników na temat metod phishingowych. Moim zdaniem koszty kursów edukujących pracowników w kwestii cyberbezpieczeństwa będą rosły szybciej niż koszty włamań. Powinniśmy zrobić coś, aby szkolenia były lepiej przeprowadzane – powiedział profesor Vishwanath podczas swojego wystąpienia.

Czytaj też: Wywiad USA wskazuję największych graczy w cyberprzestrzeni