Złudzenie bezpieczeństwa

Kategoria: Felietony
Opublikowano: wtorek, 18, kwiecień 2017 07:30
Grzegorz P. Kubalski

Nikt nie zostawia otwartych na noc drzwi do urzędu – słusznie przyjmując, ze stanowiłoby to poważne zagrożenie dla bezpieczeństwa. Repertuar fizycznych środków ochrony jest zresztą znacznie szerszy. W wielu urzędach do dziś dnia zabezpiecza się drzwi staromodnymi plastelinowymi plombami, a okna parteru są przezornie zabezpieczone kratami. Obawiam się jednak, że podejście „mój urząd – moją twierdzą" niekoniecznie rozciąga się na bezpieczeństwo informatyczne.

W ubiegłym tygodniu w Sejmie odbyła się konferencja poświęcona zagadnieniom cyberbezpieczeństwa w jednostkach samorządu terytorialnego. Kilkudziesięcioosobowej frekwencji nie można uznać za jakiś wielki sukces – nawet uwzględniając fakt, że był to okres przedświąteczny, z samej swojej natury ciężki dla samorządowców. Liczba uczestników była raczej wynikiem poziomu świadomości, czy raczej braku świadomości cyberzagrożeń w środowisku samorządowym.

A jest to objaw bardzo niepokojący. Przeważająca część incydentów bezpieczeństwa nie jest bowiem związana z jakimiś szczególnie wyrafinowanymi zabiegami informatycznymi, tylko z wykorzystaniem najsłabszego ogniwa wszystkich systemów – człowieka. Człowieka, który czasami nie myśli współczesnymi kategoriami; człowieka, którym bardzo łatwo w niektórych przypadkach manipulować. Kilka przykładów.

Corocznie podawany jest ranking najpopularniejszych haseł. I corocznie podobne zajmują pierwsze miejsca. Za rok 2016 były to kolejno: 123456 (17% przypadków!), 123456789, qwerty, 12345678 i 111111. Humorystycznie w tym kontekście brzmi informacja, że zauważalny jest wzrost świadomości użytkowników komputerów. Dowodem na to jest rosnąca popularność hasła… 123qwe. Iloma takimi hasłami zabezpieczone są dane na urzędowych komputerach?

Pomijam już te przypadki, w którym monitor jest ozdobiony kolorowymi karteczkami z hasłami do poszczególnych programów. Co prawda do ich odczytania konieczna jest przynajmniej jednokrotna obecność w pokoju, ale ilu klientów urzędu przez taki pokój się codziennie przewija?

Teoretycznie wiemy, że nie należy otwierać załączników do maili pochodzących z niezaufanego źródła. Tyle tylko, że gdy trafia się mail, z którego treści wynika iż dział księgowości prosi o zweryfikowanie poprawności naliczenia nagrody (w załączniku oczywiście) – ile osób sprawdza poprawność maila nadawcy? Zwykle perspektywa gratyfikacji finansowej wyłącza nam czujność na tyle, że załącznik bezkrytycznie otwieramy. A stąd droga do zainfekowania całej sieci gotowa.

Oczywiście metod dostania się do pożądanych danych jest znacznie więcej. Poprzez słabo zabezpieczone sieci łączności bezprzewodowej, poprzez odpowiednio (co nie znaczy – bardzo skomplikowanie) spreparowane PEN-drive'y, itd. Sytuację dodatkowo pogarsza fakt, że pensje w sektorze publicznym są niekoniecznie atrakcyjne dla osób z wykształceniem informatycznym. To z góry pogarsza sytuację urzędów, które niekoniecznie dysponują najlepszymi kadrami, a stanowisko ds. bezpieczeństwa urzędu zajmuje ktoś obeznany z zagrożeniami powszechnymi ćwierć wieku temu, a nie dzisiaj.

Konieczna jest zatem praca nad poniesieniem poziomu świadomości urzędników samorządowych, a w jeszcze większym stopniu – osób zarządzających poszczególnymi jednostkami samorządu terytorialnego, w zakresie zagrożeń cybernetycznych. Zwłaszcza, że przestają one być tylko teorią, czy też ograniczają się do utraty jakichś danych z punktu widzenia urzędu mało istotnych. Pojawiają się już bowiem pierwsze przypadki okradzenia jednostki samorządu terytorialnego z niemałych pieniędzy. Warto zatem z wyprzedzeniem zadbać o cyberbezpieczeństwo – chyba że chcemy by nasza jednostka była kolejna.