

MANAGEROWIE IT ZBYT OPTYMISTYCZNIE OCENIAJĄ BEZPIECZEŃSTWO SWOICH FIRM

W środę 20 września tego roku, odbyła się prezentacja raportu sporządzonego na zamówienie Intela. Przebadano w nim duże przedsiębiorstwa w 4 państwach: Polsce, Czechach, Rumuni oraz na Węgrzech. Na tym samym spotkaniu zaprezentowano najnowsze rozwiązanie firmy Intel w dziedzinie bezpieczeństwa czyli wieloskładnikowy system uwierzytelniający, który znajduje się poniżej systemu.

Podczas prezentacji raportu Intela Bezpieczeństwo IT w dużych firmach w Polsce w 2016 roku, jako pierwszy zabrał głos Krzysztof Jonak, dyrektor Intela w regionie Europy Środkowo-Wschodniej. Powiedział on, że dla Intela zawsze bezpieczeństwo odgrywało istotną rolę. W firmie wciąż wierzy się w tzw. Prawo Moore'a, mówiące o tym, że liczba tranzystorów w układzie elektrycznym podwaja się co 18-24 miesiące. Obecnie Intel wytwarza swoje procesory w technologii 14 nanometrów.

Zmienia się także wizja działań firmy, która przestaje być przedsiębiorstwem stricte komputerowym a coraz częściej zajmuje się Internetem rzeczy czy chmurą obliczeniową. Istotne dla firmy, staje się także również zarządzanie danymi. W tym sektorze widać w ostatnim czasie duży wzrost działań firmy teleinformatycznych. Jednocześnie widać nadchodzący trend w postaci autonomicznych samochodów czy systemów pozwalających na automatyczne przeważanie danych. Widać to choćby ze względu na powstanie nowoczesnych centrów danych w niektórych regionach świata. Krzysztof Jonak zasugerował podczas swojego wystąpienia, że w przyszłości bardzo istotne będzie wykorzystanie Big Data oraz analityki biznesowej w strategiach firm oraz organizacjach rządowych.

Intel inwestuje również w rozwój 5G świadomy, że jest to jednak narzędzie przyszłości. Według niego, przeciętny użytkownik średnio przesyła 1 GB danych w ciągu całego dnia. W momencie kiedy na rynku pojawią się autonomiczne samochody, każdy z użytkowników będzie powodował ruch na poziomie od 3 do 5 gigabajtów danych na minutę. Firma Intel zauważa jeszcze inne trendy, jak wykorzystanie wirtualnej rzeczywistości oraz rozszerzonej rzeczywistości w firmach. Oprócz tego w niedługim czasie, według Jonak możemy spodziewać się wykorzystania kamer trójwymiarowych, które pozwolą na lepszą pracę dronów np. podczas akcji ratunkowych.

Krzysztof Jonak zwrócił również uwagę na konieczność odpowiedniego zabezpieczenia danych. W innym wypadku ludzki strach przed utratą danych może spowodować niechęć do korzystania z nich. Druga część spotkania dotyczyła raportu sporządzonego na zlecenie Intela i przygotowanego przez Ipsos. W badaniu wzięło udział 80 respondentów z Polski, 50 z Rumunii, 70 z Węgier i 50 z Czech reprezentujących duże firmy zatrudniające ponad 150 osób. Większość polskich managerów IT pozytywnie oceniła poziom bezpieczeństwa w ich firmach, średni uzyskany wynik to 7,71/10.

Główne wyzwania dla bezpieczeństwa to poszerzenie się spektrum urządzeń i systemów, które mogą być celem ataków. Są to m.in. urządzenia mobilne, inteligentne zegarki czy urządzenia Internetu Rzeczy. Problemem w firmach są także działy IT, które odpowiadają za kompleksową ochronę całej infrastruktury IT, która jest w wielu firmach zbudowana z wielu elementów. Trudnościami jaki

napotykają administratorzy jest także egzekwowanie polityki bezpieczeństwa wobec prywatnych urzędów pracowników. Raport pochylił się także nad problemem wynikającym ze stosowania w polskich firmach, jednopoziomowych metod uwierzytelniających, które stosowane w bezpiecznych systemach.

Raport pokazuje, że 22 proc. przedsiębiorstw w Polsce doświadczyło poważnego incydentu naruszenia bezpieczeństwa raz w ciągu ostatniego półrocza, 5 proc. z nich uległo wypadkowi więcej niż 3 razy. Przez poważny incydent rozumiano wykrycie złośliwego oprogramowania, wyciek danych, dostęp do sieci przez nieuprawnione osoby. O bezpieczeństwie firm nie najlepiej świadczy też, że 40 proc. z nich nie ma przygotowanego scenariusza postępowania na wypadek incydentu naruszenia bezpieczeństwa. Bardzo niepokojący jest fakt, że 62 proc. przedsiębiorstw używa tylko jednego stopnia zabezpieczeń w uwierzytelnianiu użytkownika – hasła.

W rekomendacjach Intel sugeruje, że bezpieczeństwo IT musi stać się priorytetem dla wszystkich firm, jest to obszar na którym nie warto oszczędzać. Każda organizacja powinna być świadoma, że może stać się ofiarą cyberprzestępców. Jedyną niewiadomą pozostaje, kiedy nastąpi atak i jaki przyniesie skutek dla działań firmy. Dlatego też wszystkie firmy powinny opracować scenariusz awaryjny na wypadek cyberataku.

Ponadto eksperci Intela zauważają, że bezpieczeństwo IT to nie tylko oprogramowanie, ale także urządzenia i serwery. Wiele technologii pomagających zabezpieczyć dane znajduje się w urządzeniach. Twórcy raportu podkreślają ważność rozsądnego inwestowania w najlepsze technologie, które odpowiednio ochronią najcenniejsze firmowe dane. Przedsiębiorstwa powinny w skuteczny i kompleksowy sposób zabezpieczać wszystkie elementy infrastruktury. Kluczowe jest zapewnienie wymiany informacji i współpracy między poszczególnymi elementami sieci zabezpieczeń – jak pokazują raport firmy Intel.

Spotkanie zostało zakończone prezentacją Richarda Currana, dyrektora ds. bezpieczeństwa w firmie Intel. Przedstawił on zmiany, które zachodzą w środowisku bezpieczeństwa. Mówił, że coraz trudniej jest zabezpieczyć dane, których ilość rośnie w szybkim tempie. Równie trudno jest zapewnić odpowiedni poziom ochrony coraz większej ilości podłączanych urządzeń do globalnej sieci. Zmiany, które obecnie zachodzą zdecydowanie ułatwią prowadzenie działań różnej cyberprzestępców i podmiotom mające złe zamiary. Rozwiązaniem jest potraktowanie bezpieczeństwa jako części DNA swojej organizacji. Pomocne w tym może być nowe narzędzie Intela czyli wieloskładnikowy system uwierzytelniający.

Czytaj też: [Korporacje jednak dogadają się z Chinami?](#)