Cyberdefence 24

aut. Rafał Lesiecki 24.04.2018

MAŁE I ŚREDNIE PODMIOTY A CYBERBEZPIECZEŃSTWO. "UFAJ, ALE SPRAWDZAJ" [SECURETECH CONGRESS 2018]

Zaufanie, dzielenie się odpowiedzialnością, ale i możliwość sprawdzenia – to kluczowe zagadnienia we współpracy pomiędzy klientem a dostawcą usług z zakresu cyberbezpieczeństwa – uważają uczestnicy dyskusji, która odbyła się podczas SecureTech Congress 2018.

Jak zauważył Michał Możdżonek, ekspert IT, który prowadził debatę na temat bezpieczeństwa informacji w organizacji, małe i średnie przedsiębiorstwa mają problem z radzeniem sobie z cyberbezpieczeństwem, co wynika z braku zasobów ludzkich i odpowiednich środków finansowych.

Regionalna dyrektor sprzedaży firmy Fortinet Jolanta Malak podkreśliła, że podstawą budowy relacji z klientami jest jakość dostarczanych produktów i rozwiązań. – *Tak naprawdę jako dostawca dotykamy bardzo wielu wrażliwych miejsc u klienta i nie można tego realizować, kiedy po stronie klienta nie ma zaufania do tego, co robimy. Te zaufanie można budować na różne sposoby* – powiedziała Malak. Jej zdaniem sukces tak naprawdę zależy od dobrej komunikacji.

Malak zauważyła, że jej firma nie tylko występuje jako dostawca usług z zakresu cyberbezpieczeństwa, jak i współpracuje z mniejszymi podmiotami zewnętrznymi. Przy wyborze poddostawcy – mówiła dyrektor z Fortinetu – najważniejsze jest zaufanie, wiarygodność firmy, możliwości przerobowe, dostosowanie do łańcucha produkcji oraz łatwość prowadzenia komunikacji.

Czytaj też: Polski black-out? Zagrożenia dla IoT w systemach zarządzania

Dyrektor Departamentu Cyberbezpieczeństwa w spółce Exatel Jakub Syta przyznał, że jednym z trudniejszych tematów podczas negocjacji jest podział odpowiedzialności między stronami umowy.

– *Mamy dział szybkiego reagowania na incydenty i zdarza nam się, że wjeżdżamy do organizacji, w której jest bardzo poważna sytuacja. Kiedy jesteśmy proszeni do pomocy w takich przypadkach, to tak naprawdę nikt się nie interesuje, kto jest winny, kto niewinny. Cel jest jeden, konkretny: jak najszybciej pozbyć się problemu, we właściwy sposób zabezpieczyć dowody, skontaktować się z odpowiednimi organami. To jest w tym momencie kluczowe* – zauważył Syta.

Czytaj też: Chmura naturalnym elementem ewolucji w dziedzinie bezpieczeństwa IT [SecureTech Congress 2018]

Przytoczył też przypadek incydentu, którym obsługiwali pracownicy Exatela.

> *Systemy bezpieczeństwa pokazały jasno – incydent miał miejsce trzy tygodnie wcześniej, wjechali przestępcy w taki a taki sposób, wykorzystując taką a taką lukę w organizacji i już tam byli. No i tak naprawdę okazało się, że przez szereg tygodni właściwie nikt o po stronie tamtej organizacji nawet się nie zorientował, że system bezpieczeństwa podniósł alarm. To się naprawdę świeciło na czerwono. Pamiętam, że po wszystkim były przez chwilę dyskusje: dlaczego my o tym nie wiemy, czy mamy dobre technologie? Ja tak patrzę z boku i myślę: technologia zadziałała. Tak naprawdę to procesy po stronie organizacji nie zadziałały.*
>
> *Jakub Syta, Exatel*

Dr Łukasz Kister mówił z kolei, że bezpieczeństwo informacyjne jest dziś nie do końca właściwie postrzegane. W ten sposób rozumie się zazwyczaj tylko elementy związane z ochroną informacji. Tymczasem każda organizacja potrzebuje zdolności: do pozyskiwania dobrej jakości, właściwej i niezbędnej informacji, następnie do przetwarzania i ochrony tych danych, a także do dystrybucji tej informacji. – *To wszystko należy traktować jako bezpieczeństwo informacji. Zdolność do tego, by organizacja była w stanie wykorzystywać informacje jako niematerialne dobro. Do tego potrzebne są i kompetencje ludzkie, i właściwe systemy nie tylko informatyczne* – powiedział Kister.

Czytaj też: Czynności śledczo-analityczne jako część Security Operations Center [SecureTech Congress 2018]

Jak dodał, należy się zastanowić, czy jakakolwiek organizacja jest w stanie sama sobie poradzić z wyzwaniami informacyjnymi. – *Myślę, że jest to pytanie czysto retoryczne, ponieważ musielibyśmy zbudować olbrzymią organizację, która dysponowałaby niezwykłymi kompetencjami* – zauważył Możdżonek.

Czytaj też: Cyberprzestępcy używają AI w swojej działalności [SecureTech Congress 2018]