Ransomware stało się jednym z największych zagrożeń dla przedsiębiorstw. Może sięgać bardzo głęboko i paraliżować całe sieci. Wykorzystując luki w zabezpieczeniach potrafi szybko ograniczyć działanie firmy, w tym również zablokować dostęp do systemu ERP, który stanowi kręgosłup całej organizacji. Co zrobić, by ten najważniejszy system został poprawnie zabezpieczony i w jaki sposób umożliwić szybkie wznowienie jego działań w przypadku ataku?

Architektura, a nie produkty punktowe

Skuteczność działania architektury bezpieczeństwa IT w organizacji jest uzależniona od kompleksowego projektowania rozwiązań. To proces, który stale należy usprawniać i monitorować. Bezpieczeństwo systemów ERP związane jest bezpośrednio z zabezpieczeniami całej infrastruktury IT. Nie sposób zapewnić skutecznej ochrony po stronie aplikacji, jeśli mamy jakieś "dziury" na niższym poziomie. Każda firma powinna posiadać odpowiednią politykę bezpieczeństwa, czyli zbiór zasad i procedur bezpieczeństwa wraz z planem wdrożenia i egzekwowania.

Plan B

Przejdźmy teraz do rzeczy. Należy zdać sobie sprawę, że nawet najlepsze zabezpieczenia i najlepsi fachowcy nie zagwarantują nam 100%-ego bezpieczeństwa. Po drugiej stronie zawsze może znaleźć się ktoś, kto znajdzie sposób na ominięcie zabezpieczeń. Szybki rozwój organizacji i łączenie rozwiązań różnych generacji sprawiają, że szczelność tych połączeń nie jest najlepsza – pomimo systematycznej, czasochłonnej pracy, którą stale realizują działy IT. Systemy informatyczne często są więc pełne luk – załatanych, odkrytych – czekających na wykorzystanie oraz tych, które dopiero zostaną znalezione. Będąc w pełni świadomym tej sytuacji do głowy przychodzi tylko jedna rzecz – trzeba mieć plan awaryjny, który będzie mógł być wcielony w przypadku, gdy dojdzie do najgorszego.
Podstawowa sprawa to środowisko zastępcze, które w przypadku awarii czy ataku będzie mogło przejąć realizację kluczowych procesów biznesowych. Co istotne, gdy mamy do czynienia z atakiem takie środowisko powinno być uruchomione dopiero po zdiagnozowaniu i usunięciu podatności, która została wykorzystana do przełamania zabezpieczeń. Niezbyt rozsądnym rozwiązaniem byłoby stracenie również środowiska awaryjnego :). W zależności od wielkości oraz specyfiki przedsiębiorstwa awaryjne środowisko może mieć różne rozmiary. Oczywiście koszt utrzymania takiego rozwiązania może być wysoki, jednak na pewno nie będzie większy niż ewentualne straty, które zostaną wygenerowane, gdy nasza firma przestanie funkcjonować na dłuższy czas.

Warstwy zabezpieczeń

W budowie systemów ERP często wykorzystuje się architekturę wielowarstwową, gdzie dane oddzielone są od logiki aplikacji, a ta z kolei oddzielona jest od interfejsu użytkownika. Podejście takie zastosowano również w przypadku projektowania systemu Microsoft Dynamics NAV, dzięki czemu każda z warstw może mieć swój własny plan przywrócenia do pracy. Jego realizacja zależeć będzie od rodzaju i skali ataku. W najlepszym przypadku, gdy mamy bardzo dużo szczęścia, skończy się tylko na zainfekowaniu terminali użytkowników. Umożliwienie im dalszej pracy ograniczy się do przygotowania i wystawienia terminali zastępczych. Praca organizacji nie będzie zagrożona, a procesy funkcjonujące na innych warstwach będą cały czas działać. A co w najgorszym ? Nawet wielowarstwowa architektura nie uratuje nas, gdy kilka lub więcej warstw zostanie zaatakowanych. Ułatwi nam jednak przywracanie systemu. Prace będą mogły być prowadzone jednocześnie na kilku warstwach, co znacznie przyśpieszy powrót do stanu sprzed ataku.

Game Stop

Ataki typu ransomware polegają na zaszyfrowaniu danych. Zaatakowany serwer aplikacyjny w przypadku, gdy mamy zapasowy nie robi żadnego wrażenia. Co jednak, gdy wirus dobierze się do miejsca, w którym przechowujemy cenne dane? Jeśli nie posiadamy odpowiednich procedur dotyczących robienia kopii zapasowej danych oraz nie przewidzieliśmy, że taka sytuacja może mieć miejsce, niestety nie jesteśmy w stanie za wiele zrobić. Oznacza to, że w takim przypadku jedynym rozwiązaniem jest postawienie systemu od nowa. No chyba, że jesteśmy w posiadaniu dużej ilości bitcoinów i zapłacimy tzw. okup. Oczywiście taki scenariusz sprawdzi się tylko w sytuacji, gdy autorzy wirusa są „uczciwi” i odeślą nam klucz do odszyfrowania plików.

Backup na poważnie

Archiwizacja danych to podstawa. Ważna jest jednak kwestia częstotliwości robienia kopii danych oraz miejsce ich przechowywania. Trzymanie kopii zapasowej na serwerze w tej samej sieci nie wydaje się być dobrym pomysłem. Wirusy ransomware wykorzystują różne podatności i próbują zarazić jak największą liczbę ofiar. Jeśli serwer z kopią zapasową będzie miał połączenie z innym zaatakowanym komputerem istnieje bardzo duże prawdopodobieństwo, że i on zostanie zaszyfrowany. Jak sobie zatem radzić? Nie ma jednej prawidłowej odpowiedzi. W zależności od rodzaju przedsiębiorstwa oraz danych, na których operuje częstotliwość, miejsce przechowywania danych może być różne. Ważne jest jednak,

żeby dane były odseparowane lub przechowywane w inny sposób (np. backup na taśmach).

Kultura bezpieczeństwa w organizacji

Ostatnia rzecz, być może najważniejsza, to budowanie świadomości cyberzagrożeń, które obecne są w dzisiejszym świecie i edukacja użytkowników. W większości wypadków to oni są pierwszymi ofiarami. Mimo największych starań działów IT mogą zbagatelizować sprawę i ściągnąć zagrożenie. Często też użytkownicy nie są świadomi, że zainfekowanie ich komputera może skutkować nawet zatrzymaniem pracy całej firmy. Warto im zatem regularnie przypominać, aby nie otwierali załączników z podejrzanych maili. Tym właśnie sposobem ransomware rozprzestrzenia się najczęściej, atakując najbardziej podatną część naszego systemu – użytkownika.

System ERP integruje wszystkie procesy zachodzące w każdym oddziale firmy na różnych szczeblach. Optymalizuje pracę na wielu płaszczyznach – od finansów, przez zarządzanie zasobami ludzkimi po logistykę i produkcję. Dzięki temu umożliwia podejmowanie decyzji w oparciu o najbardziej aktualne informacje w czasie rzeczywistym, usprawnia i systematyzuje pracę całego przedsiębiorstwa. Kluczowe jest więc poprawne zabezpieczenie tych danych, aby w przypadku awarii lub ataku jak najszybciej podnieść działanie organizacji.

Chcesz wiedzieć więcej o tym jak dbać o bezpieczeństwo online? Napisz do nas.