Do listy niebezpieczeństw zagrażających zakładom przemysłowym coraz częściej dołączają te z zakresu cyberprzestępczości. Hakerzy jako cel ataków wybierają już nie tylko banki czy instytucje publiczne, ale również elektrownie, szpitale, fabryki czy zapory wodne. Jak podkreślają specjaliści firmy ASTOR – jedynym sposobem na uniknięcie tych zagrożeń jest dbałość o odpowiedni poziom bezpieczeństwa przemysłowych systemów informatycznych.

Celem ataków hakerów działających z pobudek finansowych są zwykle konta bankowe osób prywatnych czy przedsiębiorstw. Coraz częściej pojawiają się jednak informacje o równie spektakularnych atakach, wymierzonych w zakłady przemysłowe. Hakerzy jako swój cel obierają np. przemysłowe systemy informatyczne, odpowiadające za monitoring czy sterowanie procesów, m.in. stosowane w elektrowniach systemy SCADA. To najczęściej forma szpiegostwa gospodarczego, a uzyskane w ten sposób informacje mogą posłużyć do walki z konkurencją i czerpania konkretnych zysków z ataku.

Na liście powiązanych z działaniami hakerów zagrożeń informatycznych dla przemysłowych systemów IT i systemów z zakresu automatyki, znajdują się m.in. wirusy czy trudne do wykrycia i usunięcia przypadki malware'u zagnieżdżonego w biosach komponentów sprzętowych. Jak podkreślają specjaliści, najpoważniejszym niebezpieczeństwem są jednak w tym przypadku zaawansowane, ukierunkowane rootkity. To programy, które z założenia mają pozostać jak najdłużej niewykrywalnym elementem systemu, przy jednoczesnym zachowaniu pełnej kontroli nad nim i możliwości przesyłania informacji. Rozprzestrzeniają się nie tylko drogą sieciową, ale także m.in. poprzez przenośne karty pamięci. Jednym z nich jest np. Stuxnet, wykryty po raz pierwszy w 2010 roku robak, któremu udało się przeniknąć do systemu irańskiej elektrowni atomowej, prawdopodobnie za pośrednictwem pamięci przenośnej USB użytej nieświadomie przez pracownika jednej z firm podwykonawczych.

Podobne wniknięcie do systemu nie zawsze jest efektem działań zewnętrznych. Sporą część ataków na systemy informatyczne stanowią także ataki wewnętrzne. Rozwiązania działające w warstwie automatyki, takie jak systemy monitoringu i sterowania procesem HMI/SCADA, czy systemy klasy MES coraz częściej integrowane są z systemami biurowymi, biznesowymi, np. ERP zarządzanymi przez działy IT, więc niedopilnowanie kwestii bezpieczeństwa któregokolwiek z elementów, może przynieść dotkliwe konsekwencje.

– Aby uniknąć zagrożeń, zakłady przemysłowe powinny przede wszystkim opracować odpowiednią politykę bezpieczeństwa. Zgodnie z nią np. każdy element systemu (w tym osoba czy program) powinien mieć dostęp tylko do tych informacji i zasobów, które są niezbędne do spełnienia wyznaczonego mu zadania. Duże znaczenie mają również elementy bezpieczeństwa architektury takie jak firewall, systemy typu IDS (Intrusion Detection Systems), IPS (Intrusion Prevention Systems), czy DMZ (Demilitarized Zone). Należy także m.in. zadbać o system tworzący kopie zapasowe danych, odpowiednie oprogramowanie antywirusowe, integracje wdrażanych rozwiązań z istniejącymi już w firmie wersjami systemów i programów oraz odpowiednią aktualizację zarówno systemu operacyjnego, jak i aplikacji – także tych przemysłowych. Takie działania pozwalają zmniejszyć nie tylko ryzyko ataku, ale i nieintencjonalnej

utraty danych – komentuje Stefan Życzkowski, prezes firmy ASTOR, dostarczającej nowoczesne technologie z zakresu systemów IT i automatyki dla przemysłu.

Zdaniem specjalistów – kluczem do uniknięcia zagrożeń zewnętrznych i wewnętrznych czyhających na przemysłowe systemy informatyczne jest także umiejętność otwartego dialogu między działami IT, a działami automatyki, produkcji i utrzymania ruchu, odpowiedzialnymi za instalacje przemysłowe. Duże znaczenie mają również kroki podejmowane przez producentów oprogramowania. Przykładem jest tu choćby działalność firmy Wonderware, która do celów testowych stworzyła laboratorium bezpieczeństwa systemów – Wonderware Security Central, gdzie testowana jest zgodność wszystkich aktualizacji i poprawek systemów operacyjnych z aktualnymi wersjami jej produktów. Dzięki temu użytkownicy otrzymują informacje, jakie poprawki mogą bezpiecznie zaaplikować w systemie, a które z nich wymagają szczególnej procedury wdrażania.

Firma ASTOR jest dostawcą nowoczesnych technologii z zakresu systemów IT dla przemysłu, automatyki przemysłowej i robotyki oraz wiedzy biznesowej i technicznej dla polskich i zagranicznych przedsiębiorstw przemysłowych. Firma powstała w 1987 roku w Krakowie. Obecnie posiada siedem oddziałów w całej Polsce, m.in. w Warszawie, Poznaniu, Katowicach i Wrocławiu. Oferta ASTOR obejmuje m.in systemy sterowania General Electric i Horner APG, oprogramowanie przemysłowe Wonderware, roboty przemysłowe Kawasaki i Epson, a także ekonomiczne urządzenia automatyki własnej marki Astraada. W głównej siedzibie firmy – ASTOR Technology Park funkcjonuje pierwsza w Europie interaktywna, dostępna dla kontrahentów, studentów, przedstawicieli świata naukowego i turystów, wystawa robotyki i technologii IT – ASTOR Innovation Room, w której odbywają się testy, pokazy i szkolenia.

ASTOR jest wieloletnim członkiem Business Centre Club oraz zdobywcą wielu nagród zarówno polskich, jak i międzynarodowych, m.in. prestiżowego tytułu „Ten, który zmienia polski przemysł", Medalu Europejskiego oraz tytułu siódmego Najlepszego Miejsca Pracy w Polsce w roku 2014, w kategorii firm zatrudniających do 500 osób.

*Więcej informacji o firmie dostępnych jest na stronie: www.astor.com.pl***ASTOR**

WIĘCEJ INFORMACJI z firmy ASTOR (PRESS BOX)