Internet rzeczy i audyt IT

Rozwój i rozprzestrzenianie się technologii internetowych i komunikacyjnych (ICT) w ciągu ostatniej dekady zaowocowało gigantyczną siecią połączonych ze sobą urządzeń. Badania Gartnera obecnie szacują, że w domowych środowiskach konsumenckich jest około 3 miliardów podłączonych urządzeń. Przewiduje się jednak, że do roku 2020 będziemy mieli podłączonych i komunikujących się ze sobą prawie 21 miliardów urządzeń. Ten wzrost nie ogranicza się do tradycyjnych środowisk konsumenckich, ale obejmuje również miliony urządzeń, które są stale instalowane i wdrażane przemysłowo w obiektach takich jak fabryki, magazyny. Obecnie możliwości Internetu Rzeczy w branżach takich jak opieka zdrowotna, transport oraz handel detaliczny i logistyka zapewniają ogromne korzyści w zakresie oszczędności kosztów w prawie każdym aspekcie ich działania. Jednak, podobnie jak w przypadku przyjęcia każdej rozwijającej się technologii, IoT wiąże się z szeregiem zagadnień, takich jak akceptacja, użyteczność, bezpieczeństwo, wśród których bezpieczeństwo zwykle okazuje się jednym z najważniejszych. Wiąże się to z faktem, że przeciętnie jedna osoba może być powiązana z maksymalnie trzema różnymi urządzeniami związanymi z Internetem Rzeczy, co zwiększa szanse i możliwości uzyskania przez złośliwe osoby nielegalnego dostępu. Raport opublikowany przez Gartner Research Group wykazał wzrost o ponad 300 milionów dolarów wydatków związanych z bezpieczeństwem na IoT na całym świecie w latach 2014-2018. Ten ogromny wzrost prognozowanych wydatków na bezpieczeństwo IoT wskazuje na potencjalną lukę związaną z tymi technologie. Dlatego wymaga to szczegółowych zasad korzystania z tych technologii w organizacjach, ale co ważniejsze, wdrożenia kompleksowych rutynowych procedur audytu. Wdrożenie takich rutynowych audytów zapewni niezmiennie solidną i odporną infrastrukturę niezależnie od zmian/ulepszeń sprzętu, oprogramowania lub poprawek. Dlatego w tej części omówiono i rozwinięto nieco nowatorską koncepcję audytów w odniesieniu do IoT.

Zagrożenia związane z Internetem Rzeczy

W swojej definicji Międzynarodowy Związek Telekomunikacyjny (ITU) opisał IoT jako (i) globalną infrastrukturę dla systemów informatycznych w społeczeństwie, która (ii) umożliwia i ułatwia korzystanie z zaawansowanych usług za pomocą połączeń obiektów fizycznych i wirtualnych (iii) wspieranych przez istniejące i rozwój interoperacyjnych technologii informacyjnych i komunikacyjnych. Drugi punkt tej definicji przedstawia bardzo interesujący i unikalny scenariusz, którego dotychczas nie zaobserwowano – koncepcję połączenia obiektów fizycznych i wirtualnych w sposób interoperacyjny. Zasadniczo dodaje to warstwę wzajemnych połączeń, która praktycznie nie istniała, ponieważ obiekty, które tradycyjnie nie były uważane za urządzenia zdolne do pracy w trybie online, uzyskują teraz możliwości Internetu. Obiekty takie jak lodówki, termostaty, urządzenia zdrowotne i wiele obiektów, które wcześniej nie były przystosowane do technologii internetowej, pojawiają się w Internecie. Problemem związanym z szybkim tempem, w jakim te urządzenia ożywają w Internecie, jest brak zabezpieczeń wbudowanych w typowe urządzenia IoT. Bezpieczeństwo jest czasem refleksją po osiągnięciu pierwotnego celu komunikacyjnego urządzenia. Firma HP opublikowała raport ryzyka Internetu rzeczy oparty na analizie bezpieczeństwa urządzeń IoT w 2015 roku, zawierający kilka intrygujących statystyk. Badanie wykazało, że na listach powszechnie używanych urządzeń IoT ponad 70% tych urządzeń jest wysoce podatnych na ataki, które nie są odpowiednio zabezpieczone. Znaczna liczba tych urządzeń korzysta z niezaszyfrowanych usług sieciowych, których połączenia z chmurą i powiązanymi aplikacjami są ujawniane. To sprawia, że są podatni na proste wyczyny, takie jak człowiek w środku i tym podobne. Firma HP odkryła również, że 80% haseł używanych na tych urządzeniach to albo hasła powszechnie używane, albo to samo hasło powtarzane na wielu urządzeniach i kontach, co m.in. stwarzało więcej możliwości dla atakujących . Te luki w zabezpieczeniach są poważnym problemem w każdym modelu biznesowym, w którym te

urządzenia są używane i mogą mieć poważne reperkusje, jeśli nie zostaną odpowiednio wcześnie rozwiązane. Wszystko to pokazuje, że chociaż IoT niesie ze sobą duży potencjał i możliwości, istnieją kluczowe kwestie związane z ryzykiem, zagrożeniami, bezpieczeństwem i audytem, które należy wziąć pod uwagę. Poniżej omówiono niektóre z zagrożeń, które się pojawiają i dlatego należy je wziąć pod uwagę przy rozważaniu Internetu Rzeczy i audytu.

Prywatność

Kwestią numer jeden w kontaktach z Internetem Rzeczy jest prywatność. Dzieje się tak, ponieważ te czujniki i urządzenia znalazły się w bardzo bliskiej odległości od naszego życia i naszych osobistych przestrzeni, takich jak domy, samochody, a nawet nasze ciała, a zatem zachowanie prywatności przy wszystkich gromadzonych danych staje się kwestią nadrzędną. Żywym przykładem jest włamanie do elektronicznej niani, które miało miejsce w kwietniu 2014 roku. Intruz mógł zdalnie uzyskać dostęp do elektronicznej niani, gdy rodzina spała. Właściwie był w stanie obrócić kamerę w dowolnym kierunku, a także słychać było krzyki na dziecko i wykrzykiwanie bardzo przekleństw. To jaskrawy przykład traumatycznego naruszenia prywatności tej rodziny. W otoczeniu organizacyjnym intruz mógł skorzystać z tej drogi, aby monitorować organizację. W prosty sposób można było uzyskać informacje takie, jak kto ostatni wychodzi, kto pierwszy wchodzi do biura i ile godzin spędzonych w placówce. Nie tylko to, ale mogą być w stanie uzyskać kody dostępu do otwierania drzwi wizualnie lub za pomocą sygnałów dźwiękowych wytwarzanych podczas otwierania drzwi. Rutynowy audyt urządzeń w organizacji umożliwiłby zidentyfikowanie takich urządzeń, które są opóźnione w aktualizacji oprogramowania układowego, a tym samym zapobiegną wszelkim potencjalnym naruszeniom prywatności.

Poufność, integralność i dostępność

Poufność jest z grubsza równoważna prywatności. Jednak w tym przypadku bardzo interesują nas środki, które należy podjąć, aby zapobiegać dotarciu poufnych informacji do niewłaściwych osób. Integralność dotyczy utrzymania spójności, dokładności i wiarygodności danych przez cały cykl ich życia . Urządzenia podłączone do sieci mogą zostać przejęte, jeśli sieć zostanie naruszona, a integralność danych w tej sieci może zostać naruszona lub sfałszowana. Dostępność dotyczy tutaj utrzymania funkcjonalności, gdy jest to potrzebne użytkownikowi. W 2014 roku badanie przeprowadzone przez instytut SANS wykazało, że 375 organizacji zdrowotnych w Stanach Zjednoczonych zostało skompromitowanych w ciągu miesiąca. Intruz zinfiltrował zestaw nowych i ulepszonych jednostek obrazowania radiologicznego w połączeniu z siecią i był w stanie uzyskać dostęp do akt pacjentów i poufnych informacji (Filkins, 2014). Informacje pacjentów były na łasce intruza, który równie dobrze mógł zmienić lub zmanipulować dane, naruszając w ten sposób ich integralność. Mogli również wprowadzić do systemu błąd, który utrudniał prawidłowe funkcjonowanie jednostek obrazowania, uniemożliwiając lekarzom jego dostępność w kluczowych momentach. Audyt przeprowadzony na tej kategorii urządzeń w takich placówkach medycznych ujawni potencjalne obszary, które intruzi mogą wykorzystać i zaproponuje najlepsze sposoby postępowania. Trzeba przyznać, że niektórzy producenci mogą nie od razu dostrzegać potrzeby zintegrowanych zabezpieczeń w urządzeniach, takich jak komponenty jednostki obrazowania. Jednak gdy branża/organizacje zaczną wprowadzać standardowe procedury audytu, producenci będą zmuszeni zastanowić się, jak najlepiej zintegrować zabezpieczenia w swoich produktach, aby zapewnić zgodność z audytem.

Zarządzanie tożsamością

Jeśli użytkownik korzysta ze swojego konta w mediach społecznościowych, aby uzyskać dostęp do usługi IoT online, mogą pojawić się problemy z zarządzaniem tożsamością. W scenariuszu, w którym ich konto w mediach społecznościowych zostanie naruszone, konto/urządzenie IoT również może

zostać naruszone. Na przykład intruz może przejąć kontrolę nad bezpieczeństwem Twojego domu, gdy włamie się do Twojego konta w mediach społecznościowych, które jest połączone z inteligentnym zegarkiem lub Fitbit. Intruz może również dokonać kradzieży tożsamości, gdy uzyska dostęp do danych z konta w mediach społecznościowych, a także innych danych osobowych dostępnych na urządzeniach, na przykład informacji finansowych wykorzystywanych przez aplikacje NFC obecne w telefonach, a także inteligentne zegarki/paski. Standardowe procedury audytu w każdej organizacji zapobiegną dołączaniu do sieci podatnych urządzeń lub powiadomią administratorów sieci o urządzeniach wymagających poprawki lub aktualizacji oprogramowania układowego.

Ataki fizyczne

Atakujący mogą przeprowadzić ukierunkowany fizyczny atak na inteligentną sieć na wiele sposobów. Odcinanie zasilania lub manipulowanie wyłącznikami, instalowanie urządzeń do zagłuszania sygnału na liniach komunikacyjnych itd. to możliwe ataki fizyczne, które mogą osłabić sieć. Innym aspektem ataków fizycznych w scenariuszach, w których zezwolenia zbliżeniowe mogą być również resetowanie haseł, zmiana ustawień i przekierowywanie ruchu na serwer kontrolowany przez hakera. Z ich serwerów ataki można przeprowadzać na wiele różnych sposobów, na przykład badając oprogramowanie sprzętowe urządzenia i wykorzystując nieograniczone luki w zabezpieczeniach. Ataki lokalne mogą również występować przez Wi-Fi/Ethernet.

Ataki na infrastrukturę chmury

Umożliwienie użytkownikom używania słabych haseł, brak blokowania użytkowników po nieudanych próbach, brak uwierzytelniania dwuskładnikowego (2FA), niezabezpieczone odzyskiwanie haseł i, ogólnie rzecz biorąc, nieegzekwowanie standardowych procedur bezpieczeństwa stanowi łatwy cel dla czających się napastników. Scenariusze takie jak te niezmiennie przyciągają ataki, takie jak ataki typu brute force, ślepe ataki typu SQL injection i inne ukierunkowane ataki polegające na przechwytywaniu kont. Ostatecznie każdy udany atak pozwoli atakującemu uzyskać dostęp do urządzenia (urządzeń) i danych osobowych. W przypadku niektórych ataków, takich jak ataki typu blind SQL injection, haker może uzyskać dostęp do odczytu bazy danych konsoli i uzyskać dane logowania innych użytkowników podłączonych do infrastruktury IoT w chmurze.

Ataki złośliwego oprogramowania

Oprogramowanie zawierające złośliwe oprogramowanie przypadkowo pobrane na dowolne urządzenie może z łatwością poinformować atakującego o urządzeniach w sieci i przeprowadzić wspomniane wcześniej ataki. Byłoby tylko kwestią czasu, zanim atakujący będzie mógł użyć urządzenia, a także innych podłączonych urządzeń, do przeprowadzenia ataków, takich jak podłączone tostery, które wydobywają kryptowaluty lub inteligentne telewizory, które są przetrzymywane przez złośliwe oprogramowanie. Inspekcja IoT tych urządzeń będzie również polegać na identyfikowaniu anomalii w dziennikach i generowaniu alertów w tym zakresie.

Audyt IT

Celem audytu technologii informatycznych (IT) jest zbadanie i zbadanie kontroli zarządzania w infrastrukturze IT. Zazwyczaj po przeprowadzeniu kontroli podejmowana jest decyzja, czy systemy informatyczne prawidłowo uwzględniają trzech najemców zapewniania informacji (poufność, integralność i dostępność), a jednocześnie są odpowiednio dostosowane do celów organizacji. Inspekcja IoT ewidentnie przebiega zgodnie z wieloma już ustandaryzowanymi procedurami audytu, ale wymaga dodatkowych kroków, aby właściwie zapewnić prawdziwie wielowarstwową/warstwową infrastrukturę systemu.

Audyt IoT

Właściwe zrozumienie wyzwań stojących przed urządzeniami IoT wyjaśni, że te urządzenia IoT wymagają pewnego stopnia kontroli i standardów bezpieczeństwa. Jest to oczywiste, ponieważ ewolucja i postęp większości tych urządzeń były odmienne. W ten sposób połączenie ogromnej liczby funkcjonalnie odmiennych urządzeń w jednej sieci może potencjalnie stworzyć sieć z lukami, która jest podatna na cyberataki. Biorąc pod uwagę ich rozproszone geograficznie fabryki, urządzenia te nie zawsze są produkowane zgodnie z niezbędnymi protokołami i standardami bezpieczeństwa. Wielu producentów zaangażowanych już w produkcję innych urządzeń obsługujących Internet lub urządzeń peryferyjnych może używać tych samych procedur i standardów do budowy urządzeń IoT. Podobnie jak w przypadku powszechnych urządzeń peryferyjnych obsługujących Internet, takich jak routery, przełączniki, konsole do gier, producenci naciskali na czas lub aby sprostać gwałtownym wzrostom popytu, mogliby zwiększyć produkcję bez konieczności egzekwowania zabezpieczeń. Tak było w przypadku gier Sony i niedawno zhakowanego samochodu Jeep Cherokee nasyconego technologią podobną do IoT. W związku z tym wynik urządzeń wyprodukowanych i zbudowanych zgodnie z różnymi standardami może bardzo dobrze sugerować, że będą one podatne na ataki wspólne dla każdego urządzenia podłączonego do Internetu i prawdopodobnie inne nowo opracowane ataki. Dodatkowe ryzyko, które powoduje, że ponieważ urządzenia te w końcu stają się częścią sieci, istnieje duże prawdopodobieństwo, że te „słabe łącza" w systemie mogą potencjalnie stanowić bramę do ataku na resztę sieci, a także inne podłączone urządzenia do sieci. Omówione wcześniej luki w zabezpieczeniach, mogą stanowić poważny problem w każdym modelu biznesowym, w którym używane są te urządzenia, i mogą mieć poważne reperkusje, jeśli nie zostaną odpowiednio wcześnie rozwiązane.

Potrzeba audytu

Wraz z rozprzestrzenianiem się Internetu Rzeczy miliardy urządzeń mają być stale podłączone do ogromnie rozwijającej się sieci, a wszystko to w celu poprawy jakości życia ludzi, zmiany procesów i modeli biznesowych oraz wymyślenia na nowo całych branż. Z drugiej strony IoT ma również potencjał, aby zapewnić cyberprzestępcom punkty wejścia do sieci osobistych i korporacyjnych oraz jednostek przechowywania danych. Stanowi to jednoznacznie problem, który uzasadnia procedury audytu. Straty związane z tego rodzaju atakami były historycznie znaczące, jeśli wziąć pod uwagę przykłady takie jak Target, Sony, Home Depot i Ashley Madison. Najwyraźniej głównym wyzwaniem w obecnych i przyszłych wdrożeniach Internetu Rzeczy jest zapewnienie, że nie poszliśmy na żadne kompromisy w aspekcie bezpieczeństwa. Brak odpowiednich środków bezpieczeństwa może dać intruzom szanse na dostęp i wykorzystanie danych osobowych, które są gromadzone i przesyłane do lub z urządzenia. Dane osobowe mogą być nadużywane przez nieuprawnioną osobę i mogą skutkować kradzieżą tożsamości lub oszustwem. W niektórych przypadkach może to również stwarzać zagrożenia dla bezpieczeństwa fizycznego i publicznego. Aby osiągnąć pożądane poziomy bezpieczeństwa, systemy IoT muszą przyjąć i rozwinąć wielowarstwowe kontrole bezpieczeństwa i równowagi, które zostaną ocenione podczas audytu. Urządzenie, oprogramowanie, kanały komunikacji muszą być zabezpieczone przed manipulacją i zapewniać poufność danych. Bezpieczeństwo nie powinno być refleksją, w której warstwa ochronna jest owinięta wokół gotowego produktu. Standaryzacja branżowa i najlepsze praktyki powinny dążyć do podejścia „zabezpieczenia na etapie projektowania", w którym zabezpieczenia są wbudowane w różne warstwy urządzenia, przedstawiające kilka ścian utrudniających dostęp intruzowi. Może to przybierać różne formy, na przykład uwierzytelnianie 2F (już dziś powszechnie stosowane) lub uwierzytelnianie zbliżeniowe, które zablokuje większość zdalnie przeprowadzanych ataków. Niezależnie od bezpieczeństwa i zastosowana technika zapewniania, producent musi poczynić postanowienia umożliwiające przeprowadzenie audytów w organizacji. Mówiąc o organizacji, nawiasem mówiąc, większość urządzeń IoT nie jest faktycznie uwzględnione w

audytach bezpieczeństwa, tak jak jest obecnie. Funkcja audytu wewnętrznego może edukować organ zarządzający w zakresie przewagi konkurencyjnej, jaką może przynieść przedsiębiorstwu prawidłowo funkcjonujące wdrożenie IoT. Omówi również znaczenie, korzyści i potencjalne korzyści w zakresie oszczędności w tym zakresie. Z drugiej strony można zidentyfikować potencjalne luki w zabezpieczeniach i nadużycia oraz poradzić sobie z powiązanym ryzykiem. Idąc naprzód, można by również wdrożyć środki i kontrole zapobiegawcze, naprawcze i detektywistyczne, aby wzmocnić infrastrukturę IoT. Ta praktyka audytu staje się bardzo ważnym rutynowo potrzebnym ćwiczeniem, zwłaszcza w przypadku stałego postępu w tej dziedzinie, ponieważ związane z nią zagrożenia i podatności również zmieniają się wraz z szybką ewolucją technologii. Przeprowadzanie audytów wewnętrznych może być bardzo korzystne, ponieważ może oferować strategiczne porady kierownictwu organizacji dotyczące znaczenia, korzyści i przewagi konkurencyjnej, jaką IoT może zaoferować organizacji. Kompetentny audyt może wykazać kierownictwu organizacji, w jaki sposób można skutecznie wdrożyć IoT w codziennych procedurach operacyjnych, takich jak automatyczne śledzenie zapasów. Mogą one obejmować logistykę przychodzącą, sprzedaż i marketing, aż po wypłatę produktów. Proces audytu wewnętrznego pozwala również na konstruktywne rekomendacje i porady dla kierownictwa w zakresie wdrażania zapobiegawczych środków zapobiegawczych, detektywistycznych i skutecznych działań naprawczych. Biorąc pod uwagę niewiarygodne tempo, w jakim rozwija się IoT, nieodłączne ryzyko jest poważnym problemem, ponieważ ewidentnie na ocenę bezpieczeństwa tych systemów poświęci się zbyt mało czasu. Ponadto, ze względu na brak audytu bezpieczeństwa w IoT, organizacja nie ma możliwości ustalenia źródła i rodzaju ataku. Organizacja będzie źle przygotowana na taki incydent, co wpłynie na ciągłość działania organizacji. Aby zminimalizować ryzyko związane z korzystaniem z urządzeń IoT, organizacja musi przeprowadzić opartą na ryzyku ocenę wszystkich aktywów objętych parasolem IoT i przeprowadzić kompleksowy audyt bezpieczeństwa w odpowiednich odstępach czasu wraz z dokumentacją, testowaniem oraz raportowanie procedur ciągłości działania. Organizacja może również przeprowadzić kontrolowaną samoocenę (CSA), która pomogłaby w bezproblemowych audytach. Kontrolowana samoocena to technika oceny kontroli wewnętrznej stosowana w przemyśle do identyfikowania i zarządzania aspektami ryzyka i narażenia w organizacji. Przedstawiono mocne argumenty na jej korzyść, ponieważ identyfikuje i podkreśla obszary w organizacji z potencjalnymi możliwościami

Identyfikacja i ocena ryzyka

Każdy audyt bezpieczeństwa IT rozpoczyna się od dokładnej identyfikacji i oceny ryzyka wraz z holistyczną walidacją wpływu systemów na cele organizacji. Proces ten zasadniczo rozpoczyna się od identyfikacji ryzyka, gdzie potencjalne zagrożenia dla systemu są rozpoznane i opisane. Po identyfikacji ryzyka następuje ocena ryzyka, podczas której określa się i dokumentuje prawdopodobieństwo i konsekwencje każdego ryzyka. Pod uwagę brane są ryzyka kontroli, ryzyka wykrycia, ryzyka nieodłączne oraz ogólne ryzyko badania. Po dokładnej ocenie ryzyka audytor musi określić zakres audytu poprzez holistyczną walidację audytowanej funkcji biznesowej. Zazwyczaj przed rozpoczęciem procesu audytu uzyskuje się uprzednią zgodę kierownictwa wyższego szczebla i deleguje uprawnienia od rady dyrektorów. W organizacji może rozpocząć się procedura audytu. Przede wszystkim kluczowa jest wartość, jaką system IoT generuje dla firmy lub organizacji. System, który jest scentralizowany i bezpośrednio zintegrowany z działem produkcyjnym lub produkcyjnym organizacji, byłby bardzo krytyczny, ponieważ zasadniczo stanowi integralną część silnika napędowego organizacji. Wymaga to bardziej krytycznej oceny, aby zapewnić, że silnik produkcyjny lub produkcyjny jest wystarczająco wytrzymały, aby wytrzymać ataki, które mogą spowodować awarię całego systemu. Systemy IoT, które są bardziej peryferyjne lub zdecentralizowane, niekoniecznie wymagają takiej kontroli. Kolejnym ważnym aspektem bezpośrednio związanym z wartością systemu IoT w organizacji jest środowisko zagrożeń. Nie każdy system IoT jest podatny na konkretny atak. Systemy oparte na technologii NFC i

Bluetooth niekoniecznie muszą być podatne na zdalnie zaaranżowane ataki, takie jak wstrzykiwanie SQL, ale mogą być podatne na ataki wymagające bliskiej odległości. Dlatego wymagane jest zrozumienie tego środowiska zagrożeń i planów łagodzenia. Warto również wspomnieć, że w ostatnim czasie szkody spowodowane zagrożeniami wewnętrznymi wzywają do bliższego przyjrzenia się osobom znajdującym się na liście kontroli dostępu do systemów, ponieważ mogą one również stanowić część środowiska zagrożeń. Z przykładów takich jak Snowden i NSA doszliśmy do wniosku, że lista użytkowników z uprawnieniami kontroli dostępu skutecznie stanowi środowisko zagrożenia. Tacy insiderzy są w stanie użyć dowolnego urządzenia IoT i metody eksfiltracji do wyprowadzania danych z organizacji, które skutecznie stanowią środowisko zagrożenia. Inne ważne kwestie do rozważenia obejmują ocenę scenariuszy ryzyka i przewidywanego wpływu na biznes, kwestie prywatności i prawne, które pojawiają się podczas korzystania z systemów IoT, rodzaj informacji gromadzonych z tych systemów IoT oraz szkody, które mogą wyniknąć, jeśli dane są pozyskiwane przez intruzów. Wszystko to pozwoli audytorowi na sporządzenie bardziej ukierunkowanego planu oceny audytu, który będzie lepiej służył organizacji. Organizacje, których systemy IoT są bardziej zorientowane na klienta, będą bardziej martwić się kwestiami prywatności i kwestii prawnych; mając na uwadze, że w przypadku większej liczby organizacji produkcyjnych lub skoncentrowanych na produkcji mogą być bardziej zaniepokojeni scenariuszami ryzyka i powiązanym z nimi wpływem na biznes. Po rozważeniu tych punktów można opracować skuteczną strategię audytu w oparciu o oczekiwania dotyczące wyniku audytu.

Strategia audytu

Audytor musi mieć na uwadze interes organizacji podczas audytu systemów informatycznych. Niezależność biegłego rewidenta ma kluczowe znaczenie, aby nie miały na niego wpływu żadne czynniki, które mogłyby zagrozić badaniu. Audyt można zasadniczo rozpocząć od skupienia się na następujących aspektach systemu IoT:

Bezpieczeństwo. Jak sama nazwa wskazuje, urządzenia IoT mają na ogół pewne wbudowane możliwości łączności z Internetem, a zatem stają się tak samo podatne na ataki cyberprzestępców i haktywistów, jak laptopy, notebooki i inne urządzenia obsługujące Internet. Należy przeprowadzić dokładną ocenę podatności systemów IoT oraz zidentyfikować potencjalne czynniki ryzyka i kontrole wewnętrzne. Te luki w zabezpieczeniach, zagrożenia i kontrole muszą być dokumentowane i okresowo testowane. Dokumentacja jest niezbędna do wzmocnienia kontroli systemów IoT. Bezpieczeństwo systemów dostarczanych przez strony trzecie również musi być brane pod uwagę i regularnie kontrolowane. W audycie należy również wziąć pod uwagę dokładną analizę szyfrowania stosowanego w systemach IoT. Ponadto audytorzy muszą również zapewnić, że urządzenia te są zgodne z podstawowymi standardami bezpieczeństwa i protokołami, które zostały zdefiniowane przez odpowiednie ramy bezpieczeństwa .

Zdrowie i bezpieczeństwo. Spośród wszystkich zagrożeń stwarzanych przez urządzenia IoT niezbędne są zagrożenia związane z życiem i bezpieczeństwem ludzi. Zdrowie i bezpieczeństwo mają ogromne znaczenie w branżach takich jak opieka zdrowotna, przemysł chemiczny, zakłady produkcyjne, laboratoria, w których stosowane są inteligentne urządzenia. Przykładami takich urządzeń zdrowotnych są rozruszniki serca, defibrylatory lub inne urządzenia śledzące funkcje życiowe. Systemy te muszą zostać dokładnie przetestowane przed wdrożeniem w tych jednostkach biznesowych. Oprócz tego konieczne są środki kontrolne, aby zapewnić, że wymagane procedury testowe zostaną zakończone przed poważnymi remontami, takimi jak aktualizacje, poprawki i inne zmiany, które zostaną wprowadzone do systemów IoT. Jest to bardzo ważne, gdy błędy związane z bezpieczeństwem i higieną pracy stwarzają znaczne ryzyko .

Odporność. Ponieważ urządzenia IoT są używane w kluczowych systemach, które są podatne na ataki, audytor musi ocenić istnienie mechanizmów kontrolnych, które mogłyby przywrócić systemy w przypadku awarii. Audytor musi wyjaśnić kierownictwu wyższego szczebla znaczenie ciągłości działania, odzyskiwania po awarii i reagowania na incydenty oraz aktywnie uczestniczyć w projektowaniu i testowaniu tych procedur. Procedury te mają kluczowe znaczenie dla określenia gotowości organizacji na wypadek nieszczęśliwego wypadku. Podczas testowania tych scenariuszy należy wziąć pod uwagę wszystkie kluczowe systemy, a odpowiednia dokumentacja musi być dostępna, aby zapewnić płynne przejście w przypadku zmiany. Przeprowadzanie testów w celu zapewnienia ciągłości tych procedur ma pierwszorzędne znaczenie dla określenia ich współistnienia z RPO (cel punktu odzyskiwania) i RTO (cel czasu odzyskiwania)

Monitorowanie. Podobnie jak w przypadku każdego innego systemu opartego na dostępie, istnieje pilna potrzeba środków kontrolnych, które mogą monitorować funkcjonowanie systemów IoT. Należy przeprowadzać częste testy, aby upewnić się, że kontrole działają zgodnie z oczekiwaniami. Każdy wyjątek lub błąd, który wystąpi w systemie, musi zostać pomyślnie zarejestrowany. Nagrania te mogą przybierać formę dowolnego rodzaju logowania dostępnego w systemie. Logowanie oczywiście należało do przeszłości i nadal jest ogromnym atutem podczas audytów. Porównywano go do partnera administracyjnego, który jest zawsze w pracy, nigdy nie narzeka, nigdy się nie męczy i zawsze jest na bieżąco. Odpowiednio poinstruowany, taki partner może podać szczegółowe informacje na temat czasu i miejsca każdego zdarzenia, które miało miejsce w sieci lub systemie. Instytut SANS identyfikuje różne poziomy rejestrowania, takie jak debugowanie i informacje, powiadomienie, ostrzeżenie, błąd, krytyczny, alert i awaryjny w tej kolejności ważności. Biorąc pod uwagę bardziej proaktywną postawę, kontrole prewencyjne muszą być konsekwentnie utrzymywane i mogą być testowane za pomocą testów penetracyjnych, aby zapewnić ich sprawność. Podobnie kontrole detektywistyczne muszą rejestrować każdy nielegalny dostęp do systemu, a kontrole naprawcze muszą pomyślnie przywracać utracone dane.

Zarządzanie aktywami. Audytor musi przywiązywać odpowiednią wagę do pozyskiwania i klasyfikacji zasobów Internetu Rzeczy, które są używane w organizacji. Podczas klasyfikacji tych aktywów i przesyłanych przez nie danych należy przeprowadzić całościową ocenę opartą na ryzyku. Urządzenia te muszą również zawierać wystarczającą ilość szyfrowania, aby utrata zaszyfrowanych danych nie stanowiła poważnego zagrożenia dla organizacji. Ma to ogromne znaczenie, ponieważ niedawno US HealthWorks ucierpiało z powodu naruszenia danych przez niezaszyfrowany laptop, który został utracony. Zdecydowanie głównym priorytetem powinno być zaostrzenie środków bezpieczeństwa w zarządzaniu aktywami.

Zarządzanie zmianami. Podczas aktualizacji/zmiany systemu ze starszego na ulepszony należy zadbać o płynne przejście. Nowo zastosowany system musi ograniczać ryzyko, które prawdopodobnie nękało dotychczasowe systemy, nie naruszając jednocześnie krytycznych mechanizmów kontrolnych. Ponieważ urządzenia IoT drugiej generacji zaczną zjeżdżać z linii montażowych i fabryk, konieczne będzie zapewnienie, że ich integracja z organizacją w większym stopniu przyczyni się do złagodzenia istniejących luk i podatności. Ze względu na napięte harmonogramy niektóre starsze systemy SCADA (kontrola nadzorcza i akwizycja danych) przechodzą ograniczoną liczbę testów i nie osiągają kompromisu między konkretnymi środkami bezpieczeństwa a sprawnym codziennym funkcjonowaniem. Funkcje bezpieczeństwa okazują się albo zbyt rygorystyczne i spowalniają płynne działanie, albo niewystarczająco rygorystyczne, aby promować solidną funkcjonalność, a tym samym dopuszczając luki i luki w zabezpieczeniach. Przykład takiej nieudanej próby został zaobserwowany w przypadku próby systemu Windows 7 w celu wyegzekwowania prywatności i bezpieczeństwa w całym

systemie. Dlatego też, zanim będą mogły zostać wdrożone w całej firmie, konieczna będzie dokładna ocena wszelkich nowych urządzeń i systemów IoT.

Przypadki użycia IoT w audycie IT

Szybkie innowacje możliwe dzięki IoT konsekwentnie przesuwają granice tego, jak wchodzimy w interakcję z technologią. Bezpośrednim skutkiem tego jest fakt, że organizacje widzą nowe, niestandaryzowane formy technologii wchodzące do ich sieci. Powoduje to powstawanie nowych scenariuszy mających wpływ na bezpieczeństwo, na które organizacja nie jest odpowiednio przygotowana, ponieważ nie istniały wcześniejsze standardy organizacyjne w tych obszarach. Poniżej wymieniono trzy przypadki użycia, w których wykorzystanie audytu IT byłoby przydatne w zapobieganiu lub wykrywaniu ewentualnych luk w zabezpieczeniach Internetu Rzeczy.

Przynieś własne urządzenia

Pierwszy przypadek użycia będzie dotyczył scenariusza Bring Your Own Device, w szczególności urządzeń ubieralnych ze względu na ich rosnącą popularność i rozszerzające się możliwości. W zależności od marki inteligentne zegarki mogą przeglądać Internet, synchronizować się z pocztą e-mail, pisać notatki, nagrywać głos, a nawet robić zdjęcia. Ulepszone funkcje tych urządzeń do noszenia pozwoliłyby na łatwiejsze szpiegostwo korporacyjne ze względu na możliwość wykonywania małych bitów danych ukrytych w zegarku. Innym potencjalnie niebezpiecznym scenariuszem byłoby zhakowanie inteligentnego zegarka za pośrednictwem funkcji internetowej lub ataków opartych na technologii Bluetooth. Wirus mógł nieświadomie zostać przeniesiony do biura firmy, gdzie następnie mógł rozprzestrzeniać się po podłączeniu zegarka do komputera służbowego lub innych urządzeń w biurze.

Czytniki liczników elektronicznych

Następny przypadek użycia będzie dotyczył idei czytników liczników elektronicznych. Licznik elektroniczny ułatwia śledzenie kosztów mediów w firmie, ale wiąże się z własnymi zagrożeniami. Jeśli osoba postronna będzie w stanie uzyskać dostęp do tych liczników, będzie mogła monitorować ruch w całym budynku lub firmie. Złośliwy agent może ustalić, kiedy określony obszar będzie najmniej zaludniony, a następnie wykorzystać socjotechnikę, aby przejść przez ten obszar. O wiele łatwiej jest oszukać jedną lub dwie osoby za pomocą technik socjotechnicznych niż całą grupę ludzi. Ponadto czynnik, który ma spowodować śmiertelne szkody, może przekierować przepływ gazu do skoncentrowanych obszarów w budynku, co może spowodować zagrożenie pożarowe. Znalezienie sposobów na odcięcie dopływu powietrza do tych obszarów budynków może mieć podobny śmiertelny wpływ na ludzkie życie.

Inteligentne interfejsy parkowania

Innym przypadkiem użycia mogą być inteligentne parkometry i ich połączenia z Wi-Fi w budynkach lub organizacjach. Inteligentne parkometry w konkretnym budynku będą połączone z głównym interfejsem, który może dostarczyć przyjeżdżającym kierowcom informacji o tym, gdzie dokładnie dostępny jest parking w tym budynku. W takim scenariuszu przyjeżdżający kierowca może szybko wysłać zapytanie do interfejsu parkingowego budynku, aby uzyskać informacje o dostępnym parkingu w tym budynku. Na przykład pojazd mógł właśnie wyjechać z miejsca parkingowego na poziomie 1 27, udostępniając to miejsce w interfejsie parkingowym budynku. Nadjeżdżający pojazd nie musiałby wjeżdżać na poziom 5, aby znaleźć miejsce parkingowe. Dodatkową korzyścią tego interfejsu byłoby automatyczne tagowanie samochodów pracowników. Tak więc pracownicy nie potrzebowaliby już fizycznego tagu do parkowania, ale mogliby korzystać z tagów RFID lub ewentualnie podłączyć

samochodowy system komputerowy do inteligentnej sieci parkingowej, która równie dobrze mogłaby być hostowana za pośrednictwem intranetu organizacji. Pierwszym problemem, który może się w tym przypadku pojawić, jest atak typu „odmowa usługi" (DoS), w którym atakujący lub złośliwy agent może włamać się do systemu i oznaczyć puste parcele jako zajęte, odmawiając w ten sposób legalnym użytkownikom usługi parkowania. Sytuacja staje się bardziej krytyczna, jeśli atakujący może połączyć się z intranetem organizacji i wydobyć cenne informacje o organizacji lub trywialne informacje, takie jak pojazd, którym kieruje dyrektor generalny. Istnieje wiele różnych konsekwencji, które mogą się z tym wiązać, w szczególności potencjalna utrata cennych informacji. Organizacje, które posiadają lub współdzielą interfejsy inteligentnych sieci parkingowych, musiałyby współpracować w celu ustanowienia wspólnych standardów w celu zwiększenia bezpieczeństwa, a w konsekwencji procedur audytu.

Ochrona sieci biznesowej

Rząd utworzył Federalną Komisję Handlu (FTC) w celu ochrony konsumenta przy zakupie produktów i usług1. Są niezależną agencją i jako takie nie mają bezpośredniego autorytetu ani przewagi w egzekwowaniu swoich pomysłów w określonej branży. Zamiast tego wymyślają swoją wersję rozwiązania opartego na najlepszych praktykach, na przykład w przypadku zabezpieczania Internetu Rzeczy, a następnie zalecają, aby branża przyjęła te praktyki w celu rozwiązania problemów związanych z bezpieczeństwem i prywatnością, a wszystko to w celu ochrony konsumenta . FTC rozumie, że na przykład IoT ma ogromny potencjał w zakresie innowacji komunikacyjnych i chciałaby, aby sieć się rozwijała, ale rozumie również, że użytkownicy muszą w nią wierzyć, aby mogli z niej korzystać. Oczywistym dylematem jest to, że chociaż wierzą w znaczenie tego zabezpieczenia, nie mają możliwości bezpośredniego egzekwowania prawa przez firmy z branży. W związku z tym postanawiają być bardziej przekonujący w swoim podejściu, publikując raporty przedstawiające najlepsze praktyki i organizując warsztaty, aby rozpowszechniać swoje pomysły. Choć wydaje się to świetne, niektóre z pomysłów FTC są w rzeczywistości dość podstawowe (Federal Trade Commission i inne, 2015). Fakt, że te rozwiązania jeszcze nie istniały, jest symptomem nowego zainteresowania sieci IoT. Na przykład jednym z rozwiązań jest zapewnienie, aby bezpieczeństwo było częścią pierwszego etapu projektowania produktu, a nie tylko po namyśle. Łatwo byłoby nam po prostu winić producenta za to, że nie robi wystarczająco dużo, aby chronić prywatność swoich klientów. Jednak konsument nie znajdzie na rynku wielu produktów, które zostały wykonane tak, aby były odporne na manipulacje.

Tradycyjne środki bezpieczeństwa

Inną najlepszą praktyką dla firmy jest minimalizowanie danych gromadzonych przez tę sieć lub powiadamianie konsumentów, aby byli w pełni świadomi tego gromadzenia danych. Ludzie obawiają się zbierania danych, ponieważ „Big Data" jest głównym hasłem w mediach. O ile wszyscy gracze w określonej grupie (np. urządzenia do noszenia) nie spotkają się i wszyscy obiecują ujawnić zakres gromadzenia danych, to rozwiązanie nie zostanie potraktowane poważnie. Jeśli jedna marka ogłosi zbieranie danych, konsumenci przeskoczą z tej marki do innej marki, która nie ogłosiła zbierania danych, nawet jeśli najprawdopodobniej ich dane zostaną wyprodukowane w celu kradzieży przez hakera. Rozwiązania, które proponuje FTC, muszą być dalej rozpowszechniane, zanim zostaną zaakceptowane jako poważne odpowiedzi. Tak więc, chociaż FTC może oferować tylko podstawowe pomysły, może to ostatecznie wzbudzić wystarczającą uwagę opinii publicznej, aby wdrożyć te pomysły w przyszłych produktach w celu zwiększenia bezpieczeństwa. FTC nie może po prostu organizować warsztatów z udziałem znawców branży i oczekiwać natychmiastowej zmiany obecnych praktyk. Mają swoje raporty i informacje na swojej stronie, ale realistycznie, gdyby konsumentowi zależało na tym temacie, najprawdopodobniej zebrałby już wszystkie istotne i znaczące informacje z innego źródła. Przeciętny konsument jest po prostu świadomy korzyści, jakie może odnieść dzięki możliwości łączenia

się z większą liczbą urządzeń w domu. Istnieje wiele innych dużych firm zajmujących się zaawansowanymi technologiami, które dzielą się swoimi przemyśleniami na ten temat i wydaje się, że nie ma jednej magicznej odpowiedzi na pytanie, jak niezawodnie zabezpieczyć tę sieć. W międzyczasie po prostu rozwijamy sieć, ponieważ nie wierzymy, że hakerzy włamią się do naszych lodówek lub innych tego typu urządzeń. Podobnie jak w przypadku kradzieży karty kredytowej, nigdy nie myślimy, że nam się to przydarzy, dopóki tak się nie stanie. I nawet wtedy jesteśmy już tak zakorzenieni w tym systemie, że nie wiemy, jak postępować inaczej, więc mamy nadzieję, że problem się nie powtórzy. Mając to na uwadze, kwestionuje ostrzeżenie Federalnej Komisji Handlu przed zgubą dla rozwoju Internetu Rzeczy w związku z zainteresowaniem konsumentów i obawami o prywatność. Poprzez informowanie przeciętnego konsumenta o potencjalnych zagrożeniach i wpływie, jaki mogą one mieć na wyniki firmy, jeśli bezpieczeństwo nie jest priorytetem, FTC może pomóc zapewnić zmianę.

Nowe zasady przeciwdziałania nowym zagrożeniom

Branże, które chcą wdrożyć te urządzenia IoT, muszą być przygotowane do efektywnego zarządzania urządzeniami IoT, aby uzyskać z nich maksymalne korzyści. Muszą być przygotowani na łagodzenie wszelkich zagrożeń związanych z Internetem Rzeczy, przestrzegając określonych wytycznych i standardów. Oto kilka zaleceń dla organizacji planujących wdrożenie IoT:

* Projektowanie zabezpieczeń w systemach IoT od podstaw. Nie należy dodawać zabezpieczeń do tych systemów po ich wdrożeniu, ale należy je włączyć już na początkowych etapach rozwoju. Innymi słowy, kontrole bezpieczeństwa nie mogą być wartością dodaną do systemów IoT, ale istotną zintegrowaną funkcją.

* Zrozumienie ważnych aktywów i wartości oraz inwestowanie w ich ochronę. Firmy medyczne skupiają się na dobrym samopoczuciu pacjenta, podczas gdy organizacje komercyjne skupiają się na świetnych produktach i maksymalizacji sprzedaży. Te atuty i wartości muszą być centralnym punktem podczas planowania wdrożeń IoT.

* Zbieranie wystarczającej ilości wymaganych danych i szyfrowanie danych wrażliwych.

* Współpraca z odpowiednimi dostawcami w zakresie elementów bezpieczeństwa, takich jak zarządzanie tożsamością, analiza inteligencji zarządzania kontrolą dostępu i zarządzanie poprawkami.

* Przeprowadzenie kompleksowego audytu bezpieczeństwa systemów IoT, w tym oceny prywatności, zagrożeń i oszustw.

* Wystarczające testy przed wdrożeniem lub zmianą systemów IoT.

* Szkolenie personelu organizacji z ryzyk związanych z systemami IoT i powtarzanie go.

* Stworzenie programu świadomości bezpieczeństwa i edukowanie wszystkich członków organizacji o znaczeniu praktyk bezpieczeństwa związanych z systemami IoT

Wniosek

Nowa generacja technologii należy do urządzeń z interfejsem sieciowym, które wykonują inteligentne i złożone zadania w celu ulepszenia ludzkiego stylu życia. Ewolucja tych urządzeń pozwala im teraz wymieniać duże ilości danych, przetwarzać te dane i uzyskiwać wyniki, które pozwalają im podejmować bardzo często decyzje bez ingerencji człowieka. Niestety, ten luksus nie jest pozbawiony wad, ponieważ te sieci pełne danych stanowią bardzo atrakcyjne łóżko dla intruzów i innych umysłów o złych intencjach. W tym rozdziale podkreślono i omówiono niektóre z możliwych wynikających z tego luk oraz wykazał potrzebę rutynowego audytu. Jednak obowiązek spoczywa nie tylko na organach audytu

organizacyjnego, ale producenci muszą znaleźć sposób na włączenie kompleksowych zabezpieczeń do urządzeń IoT i systemów IoT. Powinno to odbywać się w porozumieniu z audytami na poziomie fabryki, aby zapewnić zgodność z wyznaczonymi normami. Krótko mówiąc, bezpieczeństwo zarówno na poziomie urządzenia, jak i systemu powinno być integralną częścią ich procesu budowy, po którym następują powtarzające się audyty, aby zapewnić spełnienie standardów. Ustanowienie procedur audytu dla urządzeń IoT może wydawać się daleko idące, ponieważ urządzenia te obejmują szeroki wachlarz kategorii, jak pokazano w rozdziale. Istnieją już jednak podstawowe zasady dotyczące audytu urządzeń wymieniających dane w dzisiejszym świecie. W podobny sposób można łatwo odnieść się do rygorystycznych procedur audytu, podobnych do powszechnie znanych i powszechnie akceptowanych, takich jak procedury testów penetracyjnych lub infrastruktura BYOD. Adaptacja i modyfikacja tych już istniejących technologii bez wątpienia zapewni zgodność na każdym poziomie społeczeństwa, od domów po miejsca pracy. Obecnie dostępna technologia posiada już narzędzia i możliwości do wbudowanych zabezpieczeń lub przynajmniej okresowych audytów. W tym celu priorytetem nie może być inwestowanie w nowe technologie i gadżety. Bezpośrednim celem musi być przekazanie obecnych najlepszych w swojej klasie kontroli bezpieczeństwa IT, usprawnionych dla tego nowego i złożonego ekosystemu technologii, który napędza IoT.