Praktyki bezpieczeństwa urządzeń w firmie Dell

Trzy kwestie dotyczące ustanawiania zaufania do urządzeń

Eksperci ds. cyberzabezpieczeń firmy Dell wyjaśniają kluczową rolę praktyk dotyczących bezpieczeństwa urządzeń w długofalowej strategii odporności ekosystemu IT.

Autorzy
Rick Martinez
Dell, członek i wiceprezes

Eric Baize
wiceprezes ds. bezpieczeństwa produktów i aplikacji

Wprowadzenie

Na dzisiejszym zatłoczonym rynku cybernetycznym jesteśmy prawdopodobnie zalewani opcjami produktów i rozwiązań z zakresu bezpieczeństwa. Ale co, jeśli powiem, że najważniejszą częścią strategii bezpieczeństwa wcale nie są produkty zabezpieczające?

Firma Dell, jako jeden z największych producentów komputerów osobistych, często myśli o bezpieczeństwie. W ostatnich latach, obserwując katastrofalne skutki ataków ransomware i rozprzestrzenianie się złośliwego oprogramowania na poziomie oprogramowania wewnętrznego, zauważyliśmy, że urządzenia końcowe są coraz częstszym celem. Niestety, pojedyncze rozwiązania — bez względu na ich innowacyjność — nie są w stanie w pełni zapewnić bezpieczeństwa użytkownikom i danym.

Podczas ponownej oceny bezpieczeństwa istniejącego ekosystemu i poszukiwania nowych produktów warto rozważyć nie tylko to, co kupić, ale również podejście producenta sprzętu do bezpieczeństwa. Dlaczego? Choć mogłoby się wydawać, że kluczowa jest ocena samego produktu, równie istotna jest ocena dostawcy. Zaufany i doświadczony dostawca bezpiecznych komputerów PC, który rozumie całość zagrożeń, będzie w stanie wykorzystać tę wiedzę do ochrony Twojej organizacji w miarę rozwoju sytuacji. Z takim partnerem zbudujesz ekosystem bezpieczeństwa, który będzie inteligentnie łagodzić skutki nieuniknionych ataków i zapewniać długofalową cyberodporność.

O bezpieczeństwo należy dbać wcześniej, niż mogłoby się wydawać

Osoby decyzyjne w kwestiach IT i użytkownicy końcowi zazwyczaj mają kontakt z pracownikami działu sprzedaży, urządzeniami i pomocą techniczną dotyczącą produktów. Jednak w kwestii bezpieczeństwa jest to zaledwie czubek góry lodowej. Dlaczego? Można to przyrównać do bezpieczeństwa żywności. Nie sposób ocenić go wyłącznie na podstawie interakcji z kelnerem w restauracji, ponieważ

cały proces zaczyna się już w kuchni. Analogicznie, fundamenty bezpieczeństwa urządzenia muszą zostać położone na długo przed jego wyprodukowaniem, dlatego rzadko kiedy są widoczne na pierwszy rzut oka. Firma Dell poświęciła niezliczone godziny pracy inżynierskiej i wysiłku intelektualnego na zabezpieczenie środowiska IT klienta od samych podstaw — poprzez złożone procesy i protokoły, które regulują projektowanie, rozwój i dostawę każdego urządzenia. To praca, której nikt nie dostrzega, a która tworzy stabilny, ukryty fundament, pozwalający na budowę możliwie najbezpieczniejszego urządzenia. Praca, która zabezpiecza środowisko IT klienta niezależnie od tego, czy jest to sektor publiczny, wielkie przedsiębiorstwo czy mała lub średnia firma. Firma Dell wierzy w udostępnianie nowoczesnych zabezpieczeń wszystkim firmom niezależnie od ich wielkości, dlatego zależy nam na oferowaniu rozwiązań, które chronią organizację, a tym samym jej klientów.

Nasze praktyki w zakresie bezpieczeństwa urządzeń

Zastanawiając się nad zabezpieczeniami naszych urządzeń komercyjnych, skupiamy się na wpływie na bezpieczeństwo, tj. na tym, w jaki sposób urządzenie przyczynia się do ogólnego stanu bezpieczeństwa organizacji. Jak urządzenie pomaga zapobiegać atakom? Co chroni je podczas ataku? I jak zachowuje bezpieczeństwo przez cały cykl eksploatacji?

Jak można się spodziewać, stosujemy dziesiątki praktyk mających na celu opracowywanie bezpiecznych komputerów komercyjnych, które są zgodne ze standardami branżowymi oraz modelem „zero trust". Dzisiaj omówię kilka z nich w ramach trzech głównych obszarów: bezpieczny łańcuch dostaw, bezpieczny kod i bezpieczeństwo podczas użytkowania.

1. Zabezpieczamy łańcuch dostaw naszych urządzeń. Oznacza to ścisłą kontrolę zarówno łańcucha dostaw sprzętu, jak i oprogramowania – czyli łańcucha dostaw fizycznego i cyfrowego. Kontrole te pomagają zachować integralność naszych produktów na każdym etapie produkcji, montażu, dostawy i wdrażania. Dzięki temu nasi klienci otrzymują dokładnie to, co kupili — ni mniej, ni więcej. Ponadto przekazujemy te rygorystyczne wymagania wszystkim naszym dostawcom. Jednocześnie, zgodnie z modelem „zero trust" („zakładaj naruszenie") na każdym etapie procesu wdrażamy mechanizmy weryfikacyjne.

Obejmują one zaawansowane technologie, takie jak weryfikacja zabezpieczonych komponentów (Secured Component Verification*), która identyfikuje podmianę podzespołów, oraz zdalna weryfikacja SafeBIOS, która wykrywa wszelkie próby manipulacji w najbardziej uprzywilejowanym oprogramowaniu wewnętrznym i wszczyna alarm. Te i wiele innych funkcji jest wbudowanych w Dell Trusted Devices — część naszej oferty Dell Trusted Workspace. Wykorzystujemy je również w całym łańcuchu dostaw, aby zapewnić integralność wszystkich ogniw łańcucha. Dzięki temu możemy wykrywać odchylenia, zanim dotrą one do kolejnego etapu łańcucha dostaw. (* Opcjonalna funkcja dodatkowa dostępna w sprzedaży. Dostępność różni się w zależności od regionu).

To właśnie mam na myśli, mówiąc o wpływie na bezpieczeństwo. Funkcje te zostały opracowane nie dla samej innowacyjności, ale dlatego, że aktywnie rozwiązują rzeczywiste problemy naszych klientów związane z bezpieczeństwem łańcucha dostaw i zarządzaniem flotą. Nigdy nie ufaj, zawsze sprawdzaj.

Wracając do oceny dostawców, należy pamiętać, że łańcuch dostaw producenta OEM jest naszym łańcuchem dostaw — dlatego trzeba dokładnie sprawdzić stosowane przez niego praktyki. (Aby uzyskać więcej informacji na temat zabezpieczeń łańcucha dostaw, zapoznaj się z opinią, jaką przedstawiliśmy w naszym opracowaniu dotyczącym łańcucha dostaw).

2. Projektujemy i opracowujemy bezpieczne urządzenia. W tym obszarze praktyki i funkcje wzajemnie się przenikają, co pozwala nam tworzyć skuteczne — i innowacyjne — rozwiązania sprzętowe oraz oprogramowanie wewnętrzne.

Obecnie funkcje bezpieczeństwa stanowią część naszej oferty rynkowej, ale to tylko jeden z elementów układanki. Nasze produkty nie byłyby bezpieczne, gdyby ich projektowanie, rozwój i testowanie nie podlegały naszym normatywnym zasadom Secure Development Lifecycle (SDL). Podstawowym obowiązkiem wszystkich dostawców technologii jest dopilnowanie, aby sprzedawane przez nich produkty nie stwarzały nieumyślnego ryzyka dla użytkowników poprzez luki w zabezpieczeniach. Aby zapobiec atakom i zapewnić odporność naszego stosu oprogramowania zabezpieczającego, w trakcie procesu tworzenia oprogramowania przeprowadzamy rygorystyczne modelowanie zagrożeń, identyfikując ryzyko w odniesieniu do bardzo zaawansowanych założeń cyberprzestępców, a nawet stosując tę metodologię do krytycznego sprzętu.

Testujemy i weryfikujemy te założenia modelu zagrożeń w całym procesie rozwoju, współpracując z najlepszymi konsultantami testów penetracyjnych i zewnętrznymi badaczami, udostępniając im systemy Dell w celu próby ich złamania. Prowadzimy również publiczny program łowców błędów, który pozwala przetestować bezpieczeństwo naszych komputerów komercyjnych. Wykorzystujemy dane z tych raportów i przekazujemy je działowi inżynierii w celu opracowania środków zaradczych. I tak wkoło. Dlaczego to robimy? Środowiska naszych klientów wymagają wzmocnionych i zaufanych urządzeń do efektywnego działania.

3. Pracujemy nad tym, aby urządzenia były bezpieczne w użyciu. Bezpieczeństwo wymaga wspólnego wysiłku. Obecnie prawdziwe bezpieczeństwo obejmuje ochronę na poziomie sprzętu i oprogramowania wewnętrznego, a także oprogramowania. Dlatego firma Dell dokłada ogromnych starań, aby stworzyć ekosystem w pełni sprawdzonych, najlepszych w swojej klasie partnerów, którzy zapewniają ochronę przed zaawansowanymi zagrożeniami. Rozwiązania wielu z nich są bezpośrednio zintegrowane z naszymi komputerami komercyjnymi. Jednak hakerzy nieustannie opracowują nowe sposoby włamania się do oprogramowania. Z tego powodu nasze praktyki SDL mają na celu rozszerzenie ochrony po wydaniu produktu, w tym możliwość szybkiego i łatwego identyfikowania i usuwania luk w zabezpieczeniach. Firma Dell proaktywnie informuje również o nadchodzących aktualizacjach zabezpieczeń i przejrzystych zasadach wsparcia w zakresie bezpieczeństwa, aby klienci wiedzieli, jak ich produkty są chronione przez cały okres użytkowania. Aby pomóc klientom w szybkim znalezieniu informacji na temat luk w zabezpieczeniach i ich wpływie na wydane produkty, zebraliśmy wszystkie porady i powiadomienia dotyczące bezpieczeństwa w jednym miejscu. W połączeniu z dobrze udokumentowaną polityką reagowania na luki w zabezpieczeniach pozwala nam to ściśle współpracować z badaczami w miarę zgłaszania nowych luk. Skraca to cały cykl i zapewnia stały dostęp do dokładnych informacji, umożliwiając klientom ocenę i usuwanie ryzyka w ich środowiskach.

Partner ds. bezpieczeństwa, który łączy wszystko w całość

Firma Dell dąży do budowania zaufania oraz bezpiecznego, połączonego świata. Dokładamy wszelkich starań, aby zapewnić bezpieczeństwo danych, sieci, organizacji — Twoich i klientów — dzięki funkcjom zabezpieczeń starannie wbudowanym we wszystkie nasze rozwiązania. Aby dowiedzieć się więcej o naszych praktykach w zakresie bezpieczeństwa, odwiedź Centrum zabezpieczeń i zaufania firmy Dell. I jak zawsze w razie pytań skontaktuj się z przedstawicielem Dell lub naszymi specjalistami ds. bezpieczeństwa pod adresem global.security.sales@dell.com

Więcej informacji na temat Dell Endpoint Security

Skontaktuj się z ekspertem firmy Dell Technologies

Zobacz więcej zasobów

Dołącz do rozmowy, stosując #hasztag

DELL Technologies