# Budowanie zaufanego łańcucha dostaw Twojej organizacji

## Wszystko zaczyna się od krzemu

### Dlaczego bezpieczeństwo w łańcuchu dostaw jest ważne

W przeprowadzonym badaniu Aberdeen obejmującym 288 dyrektorów ds. łańcucha dostaw **wpływ na biznes kwestii związanych z bezpieczeństwem łańcucha dostaw** zajął miejsce dopiero za globalną pandemią, wycofywaniem produktów z rynku oraz ograniczeniem popytu ze strony klientów. W ciągu ostatnich 12 miesięcy:

82% respondentów wskazało, że problemy związane z bezpieczeństwem spowodowały **zakłócenia w działalności**

72% respondentów stwierdziło, że problemy związane z bezpieczeństwem doprowadziły do **utraty przychodów**

W nowoczesnym cyfrowym łańcuchu dostaw decydenci w Twojej organizacji muszą brać pod uwagę nie tylko możliwości w zakresie tradycyjnych zabezpieczeń infrastruktury informatycznej koniecznych dla jej zaufanych użytkowników, ale także możliwości niezbędne do zapewnienia bezpieczeństwa i integralności zaufanych procesów, oprogramowania i platform (sprzętu / systemu operacyjnego / systemów). **Dzisiaj budowanie zaufanego łańcucha dostaw Twojej organizacji zaczyna się od krzemu.**

### Bezpieczeństwo w łańcuchu dostaw. Część 1: Co mogłoby pójść nie tak?

W przypadku dowolnej organizacji niezależnie od wielkości tradycyjnym filarem każdej dyskusji na temat bezpieczeństwa w cyfrowym łańcuchu dostaw jest „triada C.I.A.", będącą skrótem od angielskich słów confidentality (poufność), integrity (integralność) availability (dostępność).

Poniżej przedstawiono kilka głośnych przykładów incydentów związanych z bezpieczeństwem, które doprowadziły do istotnych zakłóceń w działaniu łańcuchów dostaw w różnych branżach:

| | Przykład | Działania atakujących | Wpływ na działalność |
|---|---|---|---|
| **Zaufani użytkownicy** | Target (2013) | Użycie danych uwierzytelniających użytkownika wykradzionych od dostawcy | naruszenie bezpieczeństwa 40 mln kart płatniczych, 70 mln rekordów klientów |
| | Home Depot (2014) | Użycie danych uwierzytelniających użytkownika wykradzionych od dostawcy; zainstalowanie złośliwego oprogramowania na terminalach w punktach sprzedaży | naruszenie bezpieczeństwa 50 mln kart płatniczych |
| **Zaufane procesy** | SolarWinds (2020) | Wstrzyknięcie złośliwego kodu do komercyjnego rozwiązania do zdalnego monitorowania i zarządzania infrastrukturą | Nawet 19 tys. klientów narażonych na nieautoryzowany dostęp |
| | Accellion (2020) | Wykorzystanie wielu luk w zabezpieczeniach typu zero-day w komercyjnej aplikacji do udostępniania plików | Ujawnienie prywatnych danych setkom klientów i milionom użytkowników indywidualnych |
| | Kaseya (2021) | Wykorzystanie luki w komercyjnym rozwiązaniu do zdalnego monitorowania i zarządzania infrastrukturą | > 70 dostawców usług zarządzanych i nawet 1 500 ich abonentów narażonych na ataki ransomware |
| **Zaufane oprogramowanie** | Apache Struts (2017) | Wykorzystanie nienaprawionych luk w otwartoźródłowym oprogramowaniu aplikacji sieci Web | Naruszenie bezpieczeństwa prywatnych danych finansowych w Equifax należących do 143 mln osób |
| | Apache Log4j (2021) | Luka w zabezpieczeniach narzędzia do logowania typu open source umożliwiająca atakującym zainstalowanie złośliwego oprogramowania, przejęcie kontroli lub kradzież danych | Niezliczone aplikacje wdrażane przez tysiące zagrożonych organizacji |

**Poufność** odnosi się do systemów, aplikacji i danych udostępnianych tylko uprawnionym użytkownikom lub systemom.

**Integralność** odnosi się do systemów, aplikacji i danych, które pozostają bez zmian, z wyjątkiem celowych zmian dokonywanych przez uprawnionych użytkowników lub systemy.

**Dostępność** odnosi się do systemów, aplikacji i danych udostępnianych uprawnionym użytkownikom lub systemom tylko wtedy, gdy są potrzebne.

### Bezpieczeństwo w łańcuchu dostaw. Część 2: W jaki sposób Twoje serwery mogą stać się fundamentem zaufania

**60%**

Badanie Aberdeen dotyczące inicjatyw w zakresie modernizacji IT przeprowadzone na 304 organizacjach pokazało, że **3 na 5 (60%) organizacji planuje wymienić swoje serwery w ciągu najbliższych 2 lat;** typowy cykl wymiany serwerów wynosi około 4 lat.

**Nr 2**

**Zarządzanie ryzykiem związanym z bezpieczeństwem** było drugim najważniejszym czynnikiem decydującym o bieżących inwestycjach w modernizację infrastruktury informatycznej, ustępując jedynie zachowaniu konkurencyjności.

Kolejna wymiana serwerów w Twojej organizacji stwarza doskonałą okazję do zaplanowania bezpieczeństwa i integralności u samych podstaw Twojego zaufanego łańcucha dostaw.

**Czy Twoje serwery są chronione przed wprowadzaniem nieautoryzowanych zmian podczas uruchamiania, aktualizacji i wykonywania operacji?**

Do niedawna nie poświęcano zbyt wiele uwagi ochronie integralności serwerów podczas uruchamiania, aktualizacji i wykonywania operacji. To się radykalnie zmieniło począwszy od 2018 roku, wraz z ujawnieniem głośnych ataków na luki w zabezpieczeniach platform, takich jak Meltdown i Spectre , które mogą występować „poniżej systemu operacyjnego".

Meltdown i Spectre (2018): Okazało się, że prawie każdy chip komputerowy wprowadzony w ciągu ostatnich 20 lat miał luki w zabezpieczeniach, które mogą ujawniać dane osobowe lub hasła z pamięci jądra, z dużym prawdopodobieństwem ich udanego wykorzystania.

Czołowi dostawcy rozwiązań projektują obecnie zaawansowane funkcje zabezpieczeń na swoich platformach już od samego początku, aby zmniejszyć prawdopodobieństwo wystąpienia naruszeń związanych z integralnością w całym ich naturalnym cyklu życia – na przykład w celu:

**zabezpieczenia** integralności serwerów na wielu różnych poziomach, w tym BIOSu, oprogramowania sprzętowego, poświadczeń i kluczy szyfrowania, a także sprzętu fizycznego

**wykrywania** nieautoryzowanych zmian i złośliwych cyberataków

**przywracania** , w razie potrzeby, BIOSu, oprogramowania sprzętowego i systemu operacyjnego do znanego dobrego stanu

**bezpiecznego** ponownego wykorzystywania lub wycofywania serwerów poprzez trwałe usunięcie danych i zresetowanie atrybutów zabezpieczeń

### Czy Twoje serwery są chronione przed wprowadzaniem nieuprawnionych zmian od momentu ich wyprodukowania do czasu, gdy staną się integralną częścią infrastruktury łańcucha dostaw Twojej organizacji?

W 2019 r. dostrzeżenie ryzyka szpiegostwa i potencjalnego sabotażu komunikacji, infrastruktury krytycznej i gospodarki cyfrowej skłoniło kilka rządów do nałożenia zakazu korzystania z niektórych urządzeń telekomunikacyjnych producentów zagranicznych (np. sprzętu sieciowego 5G chińskiej firmy Huawei Technologies).

Wiodący dostawcy rozwiązań oferują obecnie również wyspecjalizowane usługi zapewniające krajowe źródła zaopatrzenia, produkcję i pochodzenie serwerów zgodnych ze standardami branżowymi – wytwarzanych przez sprawdzonych pracowników w bardzo bezpiecznych obiektach na terenie kraju – które zawierają zaawansowane funkcje zabezpieczeń wymienione powyżej.

### W jaki sposób zaufany łańcuch dostaw i usługa optymalizacji bezpieczeństwa serwerów firmy HPE mogą pomóc Twojej organizacji w zbudowaniu solidnych podstaw zaufania

Aby dowiedzieć się więcej na temat sposobu, w jaki Twoja organizacja może zbudować zaufany łańcuch dostaw od samego początku, odwiedź stronę

**www.hpe.com/security/compute ▸**



ABERDEEN STRATEGY & RESEARCH

Hewlett Packard Enterprise