

Wyprzedzanie zagrożeń dla bezpieczeństwa

Ed Tittel

SPIS TREŚCI

Chmura zmienia wszystko... łącznie z zabezpieczeniami	2
Jak HPE (z partnerami) może zabezpieczyć IT	3
Zabezpieczenia HPE zaczynają się od serwerów.....	3
Rozwiązania bezpieczeństwa HPE.....	4
Więcej niż rozwiązania: fachowe doradztwo.....	4

W NINIEJSZYM ARTYKULE

W tym krótkim opisie technicznym przedstawiono, w jaki sposób firma HPE i jej partnerzy pomagają małym i średnim firmom uniknąć problemów związanych z bezpieczeństwem. Firmy takie muszą być w stanie identyfikować zagrożenia i potencjalnie niebezpieczne luki w zabezpieczeniach, szeregować je według wagi oraz opracowywać plany ograniczania ryzyka i eliminacji nieprawidłowości. Wymaga to ciągłych, nieustannych wysiłków, aby nadążyć za ciągle zmieniającym się krajobrazem zagrożeń.

Najważniejsze kwestie:

- Dostosowanie strategii bezpieczeństwa do celów biznesowych
- Wypracowywanie kultury biznesowej nastawionej na bezpieczeństwo
- Monitorowanie płaszczyzn ataku i aktywne zapobieganie działaniom hakerów

W przypadku cyberbezpieczeństwa szczególnie trafne jest stare powiedzenie: „Lepiej zapobiegać niż leczyć”. A to dlatego, że koszty „leczenia”, czyli usuwania skutków incydentu lub naruszenia bezpieczeństwa, są obecnie na tyle wysokie, że stanowią zagrożenie dla istnienia większości firm, zwłaszcza mniejszych.

Dlatego właśnie zrozumienie i przewidywanie niebezpieczeństw, jakie mogą stwarzać zagrożenia i luki w zabezpieczeniach, jest tak ważne, wręcz nieodzowne. Ostatecznie wszystko sprowadza się do zarządzania ryzykiem, które obejmuje następujące działania:

- W miarę objawiania się zagrożeń i luk w zabezpieczeniach pierwszym krokiem jest **identyfikacja** tych, które stanowią rzeczywiste ryzyko dla firmy, oraz ocena ich potencjalnych skutków i konsekwencji.
- W przypadku zagrożeń, które wiążą się z ryzykiem, konieczne jest **ich uszeregowanie**, traktując priorytetowo te, które wiążą się z najwyższymi kosztami lub najpoważniejszymi konsekwencjami.
- W przypadku zagrożeń, których ryzyko uzasadnia reakcję, firmy powinny opracować **plany ograniczania i eliminacji ryzyka**.

W praktyce, zwłaszcza w przypadku firm zbyt małych, aby powołać własny zespół ds. bezpieczeństwa, oznacza to subskrypcję usługi analizy zagrożeń i usuwania ich skutków. HPE wraz z partnerami może pomóc w takich kwestiach, w tym w identyfikacji, priorytetyzacji i usuwaniu zagrożeń w ramach kompleksowej oferty usług z zakresu bezpieczeństwa.

Chmura zmienia wszystko... również zabezpieczenia

W miarę jak organizacje wykupują subskrypcje i usługi chmury, w środowisku bezpieczeństwa pojawiają się nowe, skomplikowane wektory zagrożeń. W związku z tym konieczne jest podniesienie poziomu bezpieczeństwa oraz podjęcie kroków mających na celu poprawę cyberbezpieczeństwa i odporności cybernetycznej organizacji. Następujące działania biznesowe mogą pomóc firmom w osiągnięciu tych celów:

- **Dostosowanie strategii bezpieczeństwa do priorytetów biznesowych:** Dzięki zrozumieniu rozbieżności między priorytetami biznesowymi i dotyczącymi cyberbezpieczeństwa kierownictwo i interesariusze mogą rozpocząć koordynowanie obu strategii, aby skupić się na kluczowych priorytetach oraz odpowiednio alokować zasoby i środki budżetowe. Ważne jest, aby liderzy biznesowi osiągnęli porozumienie w sprawie priorytetów i dobrze zrozumieli profile ryzyka.

- **Wypracowywanie kultury biznesowej nastawionej na bezpieczeństwo:** Priorytetowe potraktowanie kultury biznesowej nastawionej na bezpieczeństwo jest ważnym krokiem do osiągnięcia sukcesu w świecie przesyconym niepewnością i ryzykiem. Ochrona kluczowych zasobów staje się sprawą każdego pracownika. Inwestowanie w szkolenia uświadamiające dla pracowników ma zasadnicze znaczenie, ponieważ to oni stanowią poważne źródło cyberryzyka, a ponadto wspólna walka z cyberzagrożeniami przynosi większe korzyści firmie.
- **Poznaj płaszczyzny ataku i usuń luki w zabezpieczeniach, zanim znajdą je hakerzy:** [Analiza luk w zabezpieczeniach](#), zwana również testami bezpieczeństwa lub testami penetracyjnymi, to proces testowania, którego celem jest ocena stanu bezpieczeństwa organizacji (patrz **rys. 1**). Pozwala znaleźć luki w zabezpieczeniach, zanim atakujący zdoła je wykorzystać. Proces ten dostarcza wniosków analitycznych na temat zagrożeń dla zasobów organizacji z perspektywy zewnętrznej i wewnętrznej. Pomaga również rozpoznać potencjalne nieprawidłowości w zakresie bezpieczeństwa przed przeprowadzeniem formalnej oceny zgodności lub audytu. Aby zwiększyć poziom bezpieczeństwa w organizacji, warto też opracować plany ograniczania zagrożeń. Zaangażowanie tutaj doświadczonych partnerów (takich jak HPE ze swymi partnerami) może załagodzić brak w firmie specjalistów w zakresie cyberbezpieczeństwa i wyeliminować luki w zabezpieczeniach.

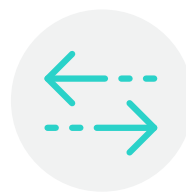
Cztery etapy testów penetracyjnych



ZBIERANIE
INFORMACJI



ANALIZA LUK W
ZABEZPIECZENIACH



SNIFFING I SPOOFING
RUCHU SIECIOWEGO



TESTY
WYTRZYMAŁOŚCIOWE

Rys 1: Cztery etapy testów penetracyjnych

Objaśnienie terminologii

Odzyskiwanie danych po awarii: dotyczy usług i systemów, które umożliwiają firmie powrót do normalnego funkcjonowania nawet w obliczu klęski żywiołowej lub całkowitej utraty dostępu i usług.

Ransomware: rodzaj złośliwego oprogramowania, które uniemożliwia firmom dostęp do systemów i danych poprzez szyfrowanie. Przestępcy żądają okupu w zamian za przywrócenie stanu sprzed ataku, ale FBI odradza płacenie okupów, ponieważ nie zawsze rozwiązuje to problem.

Wirtualizowane i konteneryzowane aplikacje i dane: aplikacje i dane, które działają w maszynach wirtualnych lub kontenerach, często w chmurze, zazwyczaj w modelu informatycznym opartym na wykorzystaniu i konsumpcji.

Od brzegu sieci do chmury: określenie zasobów obliczeniowych i danych, które mogą znajdować się w centrach danych lub serwerowniach w lokalnej sieci szkieletowej firmy, na brzegu sieci w odległych lokalizacjach terenowych lub na jednej lub kilku platformach chmurowych (np. Amazon Web Services, Microsoft Azure, Google Cloud Platform).

Środowiska hybrydowe i wielochmurowe: chmura hybrydowa to chmura łącząca lokalne i chmurowe zasoby obliczeniowe w jedno środowisko do obsługi zadań obliczeniowych. Środowisko wielochmurowe oznacza zasadniczo to samo, z tym że dotyczy dwóch lub większej liczby platform chmurowych. Większość współczesnych firm działa w hybrydowych środowiskach wielochmurowych i stara się umieszczać obciążenia i dane tam, gdzie jest to najbardziej uzasadnione z punktu widzenia kosztów, bezpieczeństwa i wydajności.

Ważne jest, aby liderzy biznesowi osiągnęli porozumienie w sprawie priorytetów i dobrze zrozumieli profile ryzyka.

Jak HPE (z partnerami) może zabezpieczyć IT

Jak szybko można się przekonać, rozwiązania HPE w zakresie cyberbezpieczeństwa są wszechstronne, innowacyjne i solidne. Jej zabezpieczenia mają bardzo rozległy zakres — od poziomu sprzętowego po użytkowników i systemy na brzegu sieci. Ogólnym celem jest gromadzenie i analiza danych bezpieczeństwa, aby nadążać za zagrożeniami, zabezpieczyć systemy i usługi biznesowe oraz doradzać klientom (i pomagać im) w zarządzaniu zagrożeniami dla bezpieczeństwa i ich minimalizowaniu.

Rozwiązania HPE w zakresie cyberbezpieczeństwa są wszechstronne, innowacyjne i solidne. Jej zabezpieczenia mają bardzo rozległy zakres — od poziomu sprzętowego po użytkowników i systemy na brzegu sieci.

ZABEZPIECZENIA HPE ZACZYNAJĄ SIĘ OD SERWERÓW

Firma HPE jest uznawana za dostawcę najbezpieczniejszych serwerów zgodnych ze standardami branżowymi. Dzięki następującym zaletom rodzina serwerów ProLiant zdobyła liczne nagrody i wyróżnienia:

- **Ochrona:** Systemy unikają narażenia na ataki na poziomie sprzętu i oprogramowania firmware dzięki technologii Silicon Root Of Trust, rozszerzeniom modułu TPM (Trusted Platform Module), wielu poziomom zabezpieczeń antysabotażowych oraz dodatkowym innowacjom HPE, takim jak oprogramowanie firmware „Integrated Lights Out” (iLO), które promują nastawienie na bezpieczeństwo.
- **Wykrywanie:** Cała gama innowacji wykrywa i odpiera zagrożenia podczas pracy, między innymi poprzez sprawdzanie integralności rozruchu, w ramach którego iLO usuwa potencjalnie (lub faktycznie) złamany kod oprogramowania firmware i w miarę możliwości zastępuje go znaną, poprawną kopią. Jeśli naprawa okaże się niemożliwa, systemy nie uruchomią się (w celu ochrony systemu przed rootkitami działającymi przed uruchomieniem i innymi podstępными atakami opartymi na oprogramowaniu firmware).

- **Odzyskiwanie:** Solidne funkcje szybkiego i łatwego przywracania i odtwarzania systemów do ostatniego znanego, dobrego, działającego stanu dzięki zabezpieczonym przed manipulacją, zaszyfrowanym kopiom zapasowym oraz bezpiecznym mechanizmom przywracania.

Zerto

W 2021 roku firma HPE sfinalizowała przejęcie firmy Zerto, która specjalizuje się w rozwiązaniach do odzyskiwania danych po awarii, odzyskiwania danych po ataku oprogramowania typu ransomware i przenoszenia zasobów między różnymi chmurami. Firma Zerto, będąca obecnie częścią HPE, oferuje ciągłą ochronę i odzyskiwanie aplikacji i danych wirtualizowanych i konteneryzowanych od brzegu sieci do chmury. Dzięki Zerto organizacje mogą w ciągu kilku minut przywrócić stan sprzed ataku, eliminując długotrwałe i kosztowne przestoje i utratę danych. Zerto zapewnia większą dostępność systemów przy znacznie niższych kosztach administracyjnych niż w przypadku starszych rozwiązań ochrony danych. Dzięki ujednoczonemu, skalowalnemu i zautomatyzowanemu zarządzaniu danymi w ramach platformy Zerto można również łatwo i bezproblemowo przenosić obciążenia robocze i dane między chmurami. Ponadto, Zerto oferuje ciągłą ochronę danych w organizacjach stosujących strategię chmury hybrydowej, z rozwiązaniem odzyskiwania danych jako usługi (DRaaS) z siecią ponad 350 dostawców usług zarządzanych. Odwiedź stronę [HPE/Zerto](#), aby dowiedzieć się, jak Twoja firma może zminimalizować niemal do zera ryzyko utraty danych i przestojów aplikacji.

ROZWIĄZANIA BEZPIECZEŃSTWA HPE

Wszystkie narzędzia, technologie i rozwiązania HPE w zakresie bezpieczeństwa wykorzystują trzy kluczowe podejścia stosowane na etapie projektowania, rozwijania, produkcji i konserwacji. Najlepiej opisać je w następujący sposób:

- **Bezpieczeństwo skoncentrowane na danych:** Środki bezpieczeństwa mają na celu przede wszystkim ochronę danych, zwłaszcza danych wrażliwych (informacje umożliwiające identyfikację osoby, czyli PII, konta i hasła, dane finansowe, zdrowotne, inne dane prawnie chronione itd.). Wiąże się to bezpośrednio z kolejnym podejściem, które skupia się na kontroli, kto i w jakim celu uzyskuje dostęp do systemów i danych.

Zaangażowanie doświadczonych partnerów (takich jak HPE ze swymi partnerami) może załagodzić brak w firmie specjalistów w zakresie cyberbezpieczeństwa i wyeliminować luki w zabezpieczeniach.

- **Bezpieczeństwo oparte na zerowym zaufaniu:** National Institute of Standards and Technology (NIST) opisuje [zerowe zaufanie](#) (ZT) za pomocą epigramu: „Nigdy nie ufaj, zawsze sprawdzaj”. Metodologia ZT skupia się na ochronie danych i usług, ale powinna również obejmować wszystkie zasoby (urządzenia, elementy infrastruktury, aplikacje oraz zasoby wirtualne i chmurowe) i podmioty (użytkowników, aplikacje, usługi i systemy). Zasadniczo ZT opiera się na założeniu, że osoby atakujące są zawsze obecne i aktywne. Dlatego nikt nie jest obdarzany bezwzględnym zaufaniem, a ryzyko dla zasobów i funkcji biznesowych jest nieustannie analizowane i oceniane. Kluczową strategią jest weryfikacja tożsamości przy każdym żądaniu dostępu, a także stosowanie „zasady najmniejszego przywileju” (ang. Principle of Least Privilege, PLP), która polega na przyznawaniu podmiotom wyłącznie tych przywilejów, które są im niezbędne do wykonywania określonych zadań.
- **DevSecOps:** Mówiąc najprościej, jest to rozwinięcie idei DevOps, która łączy programistów (i pracowników pomocniczych, takich jak testerzy, dokumentaliści i trenerzy) z personelem operacyjnym (administratorzy, wsparcie techniczne oraz technicy lub serwisanci terenowi) w jedną organizację o wspólnych celach i zadaniach. DevSecOps idzie o krok dalej i integruje personel bezpieczeństwa w całym cyklu programistycznym, dzięki czemu bezpieczeństwo jest uwzględniane na etapach projektowania, konstruowania, testowania, konserwacji i wycofywania z eksploatacji w ramach obsługi biznesowej IT.

WIĘCEJ NIŻ ROZWIĄZANIA: FACHOWE DORADZTWO

Dział [HPE Pointnext Services](#) służy pomocą małym i średnim firmom w audytowaniu, definiowaniu i doskonaleniu strategii bezpieczeństwa. Oferuje fachową pomoc w formułowaniu zasad bezpieczeństwa oraz

spełnianiu wymogów zgodności w zakresie prywatności, poufności i ochrony danych. Jego usługi mogą również pomóc firmom dysponującym ograniczonymi zasobami lub wiedzą w zintegrowaniu niedrogich i skutecznych rozwiązań zapewniających utrzymanie ciągłości działalności i odzyskiwanie danych po awarii. Pointnext tak naprawdę specjalizuje się w pomaganiu firmom w przygotowywaniu planów bezpieczeństwa, aby projekty i wdrożenia zabezpieczeń znalazły swe odzwierciedlenie w rzeczywistości (i w ramach ograniczeń budżetowych). Może również zapewnić kompleksową pomoc we wdrożeniach testowych, pilotażowych i produkcyjnych. Ostatecznie Pointnext może pomóc firmom w ugruntowaniu bezpieczeństwa w całej organizacji: wśród pracowników zdalnych, na brzegu sieci, w infrastrukturze lokalnej oraz w środowiskach hybrydowych i wielochmurowych.

Zabezpieczanie łańcucha dostaw

Dla klientów z wyższymi wymaganiami dotyczącymi zabezpieczeń i scenariuszy użytkowania HPE oferuje obsługę platformy zaufanego łańcucha dostaw (TSC). Do reprezentatywnych klientów z tego łańcucha dostaw należą organizacje i agencje rządu USA oraz sektora publicznego, które muszą nabywać produkty wyprodukowane w USA z możliwością do sprawdzenia gwarancją jakości. Bezpieczeństwo jest uwzględnione w TSC na dwa ważne sposoby. Po pierwsze, takie produkty mają wzmocnione zabezpieczenia, które czynią je nawet całkowicie odpornymi na manipulacje. Po drugie, HPE nadzoruje cały łańcuch dostaw, zatwierdza wszystkie części, kontroluje montaż oraz zabezpiecza (i chroni przed manipulacją) zapakowane towary do momentu przyjęcia dostawy przez klienta.

[Projekt Aurora](#) obejmuje kompletną architekturę bezpieczeństwa z nowymi, wbudowanymi i zintegrowanymi rozwiązaniami bezpieczeństwa, od poziomu struktury krzemowej. Dowiedz się, jak Projekt Aurora jest inicjowany w łańcuchu dostaw i tworzy odporny łańcuch zaufania obejmujący infrastrukturę, system operacyjny (OS), platformę programową i obciążenia robocze, nie wymagając podpisów, poświęcania wydajności ani uzależnienia się od jednego dostawcy.

Wszystkie narzędzia, technologie i rozwiązania HPE w zakresie bezpieczeństwa wykorzystują trzy kluczowe podejścia stosowane na etapie projektowania, rozwijania, produkcji i konserwacji.

HPE wraz ze swoimi partnerami oferuje szeroką gamę starannie opracowanych rozwiązań zabezpieczających, które pomagają małym i średnim firmom zarządzać ryzykiem, chronić systemy i dane oraz radzić sobie z dzisiejszym złożonym i trudnym środowiskiem bezpieczeństwa. Odwiedź stronę [Rozwiązania IT firmy HPE dla małych i średnich przedsiębiorstw](#), aby uzyskać więcej informacji. Ponadto HPE wraz ze swoimi partnerami może poprzez dział usług [Pointnext](#) zaoferować coaching, doradztwo, pomoc i usługi ułatwiające mniejszym firmom zachować bezpieczeństwo.