VEMCO SUMMIT 2025

Nowy wymiar kontroli dostępu w erze CER i NIS2

VEMCO SUMMIT 2025 ZA NAMI!

To był dzień pełen inspiracji, wiedzy i rozmów o tym, jak budować odporność organizacji w erze CER i NIS2.
Otrzymaliśmy wiele pozytywnych opinii - uczestnicy docenili merytoryczną wartość wystąpień, doskonałą organizację i praktyczne podejście do tematu bezpieczeństwa.
Dziękujemy za obecność i za energię, która sprawia, że już dziś myślimy o kolejnej edycji.
A teraz - zapraszamy do krótkiego podsumowania najważniejszych wystąpień i wniosków z konferencji.

To Vemco Summit 2025 w pigułce.

SABOTAŻ, CHAOS I DANE - NOWA TRIADA ZAGROŻEŃ DLA FIRM

Jacek Grzechowiak - RiskResponse

Dziedzictwo przeszłości a współczesne postawy wobec bezpieczeństwa.

Współczesna sytuacja w kraju, choć z pozoru spokojna, jest naznaczona przez zjawisko VUCA/BANI, które podkreśla niestabilność, niepewność, złożoność i niejednoznaczność otoczenia biznesowego. Czynniki te mają swoje korzenie w przeszłości, gdzie niski poziom poszanowania cudzego mienia oraz psychologiczne mechanizmy usprawiedliwiania czynów zabronionych były szczególnie widoczne. Społeczna akceptacja dla przestępczości oraz ograniczona skuteczność organów prawa w prewencji i karaniu sprawców dodatkowo komplikowały sytuację. Przykładem kradzież telewizorów z fabryk Sharp i Orion w Łysomicach, co uwidoczniło problem zorganizowanej przestępczości.

Ponadto, zagrożenia takie jak sabotaż, choć wydają się być reliktem przeszłości, nadal stanowią wyzwanie. W obliczu tych wszystkich czynników, kluczowe staje się zwiększenie świadomości bezpieczeństwa oraz efektywność działań prewencyjnych. Przykładem może być incydent w firmie EADS, gdzie w jednym z montowanych samolotów znaleziono przecięte kable. Przypadki sabotażu występowały najczęściej równolegle lub następczo z napięciami w relacjach pracowniczych. Dziś jednak w tej materii jest inaczej. Sytuacja zmieniła się diametralnie wraz z rozpoczęciem pełnoekranowej inwazji Rosji na Ukrainę.

Hybrydowe zagrożenia i konieczność adaptacji strategii ochrony.

W obliczu ewoluujących zagrożeń bezpieczeństwa, tradycyjne podejście do ochrony osób i infrastruktury okazuje się niewystarczające. Współczesne ataki dywersyjno-sabotażowe, zarówno w Polsce, jak i w całej Europie, wskazują na potrzebę adaptacji strategii ochrony. Hybrydowa natura obecnych konfliktów, w której granice między stanem wojny a pokoju są zatarte, wymusza na managerach bezpieczeństwa przyjęcie bardziej elastycznego i przewidującego podejścia. Oznacza to konieczność inwestowania w zaawansowaną analitykę danych i technologie predykcyjne – które mogą pomóc w identyfikacji potencjalnych zagrożeń zanim się zmaterializują – i łączenie ich z wysoko kwalifikowanymi pracownikami ochrony. Przykłady ataków na pozornie nieistotne cele, takie jak małe firmy logistyczne (Wielka Brytania) czy wiejskie sklepy (Estonia), pokazują, że sprawcy kierują się własnymi, często nieprzewidywalnymi kryteriami wyboru celów. Zrozumienie tej dynamiki jest kluczowe dla skutecznego zarządzania bezpieczeństwem w dzisiejszym złożonym świecie zagrożeń.

Ewolucja podejścia do infrastruktury krytycznej i odporności organizacyjnej.

Ostatnie pożary, które miały miejsce w naszym kraju, stanowią nie tylko poważne zagrożenie dla lokalnych społeczności i środowiska, ale również wskazują na konieczność zmiany sposobu, w jaki postrzegamy bezpieczeństwo i odporność infrastruktury. Tradycyjnie, infrastruktura krytyczna była uważana za kluczowy element w zapewnianiu bezpieczeństwa narodowego i gospodarczego. Jednak w obliczu rosnących zagrożeń, konieczne jest przyjęcie bardziej holistycznego podejścia. Przykład ostrzeżenia National Counterintelligence and Security Center (NCSC) do amerykańskich firm w Europie podkreśla, że zagrożenia mogą przybierać różne formy i nie ograniczają się jedynie do fizycznych ataków na obiekty IK, a firmy muszą być przygotowane na szeroką gamę ryzyk, co jest nieodzowne dla budowania długoterminowej odporności i bezpieczeństwa zarówno na poziomie państwowym, jak i korporacyjnym. Poglądy takie odzwierciedlają także publikacje takich szanowanych europejskich instytucji, jak: NPSA (Wielka Brytania) czy SÄPO (Szwecja). Również z naszego RCB płyną różnego rodzaju ostrzeżenia.

Nowe priorytety w zarządzaniu bezpieczeństwem organizacji.

Współczesne zagrożenia w biznesie zyskały więc nowy wymiar, który wymaga od zarządzających bezpieczeństwem gruntownej rewizji podejścia do ochrony organizacji. W obliczu rosnącej roli działań na zlecenie obcych służb specjalnych, kluczowe staje się nie tylko zrozumienie zmiennych motywacji i metod działania przestępców, ale także adaptacja własnych strategii ochronnych. Oznacza to, że organizacje muszą dokładnie analizować swoje słabe punkty, aby przewidzieć i przeciwdziałać potencjalnym atakom. W tym kontekście szczególnego znaczenia nabiera edukacja pracowników, rozwój zaawansowanych technologii ochronnych oraz współpraca z ekspertami ds. bezpieczeństwa, którzy mogą dostarczyć niezbędnego know-how. Tylko w ten sposób można efektywnie wzmacniać odporność na zagrożenia i minimalizować ryzyko związane z działalnością przestępczą na zlecenie.

BEZPIECZEŃSTWO TO NIE SPRINT, TYLKO STRATEGIA.

Wywiad z Marcinem Cylkowskim - Liderem Zespołu Rozwoju Produktów i Wiceprezesem Vemco - o odporności organizacji, NIS2, zdrowym rozsądku w bezpieczeństwie oraz o tym, dlaczego technologia musi wynikać z potrzeb biznesu, a nie odwrotnie.

Rozmawia Agnieszka Zalewska.

Firmy często traktują wdrażanie CER i NIS2 jak wyścig z czasem. Co jest największym błędem w takim podejściu?

Największy problem zaczyna się wtedy, gdy organizacja próbuje zrobić wszystko naraz - bez planu, bez analizy, bez zrozumienia, co naprawdę jest ważne. Dyrektywy nie wymagają od nas budowania fortecy, tylko racjonalności. Zgodność nie polega na tym, by w każdym miejscu zamontować czytnik biometryczny czy atestowane zabezpieczenia mechaniczne, ale by wiedzieć, które aktywa są dla nas najważniejsze, jakie ryzyka rzeczywiście im zagrażają i jakimi konsekwencjami grozi ich materializacja w kontekście incydentów mogących skutkować zaburzenie ciągłości działania organizacji. Inaczej przepalamy budżet i energię zespołu, a bezpieczeństwo pozostaje tylko na papierze.

Często podkreślasz, że technologia ma wspierać, a nie dominować nad biznesem. Co to oznacza w praktyce?

To proste: środki i rozwiązania gwarantujące bezpieczeństwo muszą być proporcjonalne do wartości chronionego zasobu, adekwatne do poziomu ryzyka i potencjalnych skutków wystąpienia incydentu. Jeżeli proces jest kluczowy - inwestujmy w jego ochronę. Jeżeli nie ma dużego znaczenia - zaakceptujmy ryzyko i nie komplikujmy życia. Takie podejście porządkuje priorytety, daje argumenty dla zarządu i sprawia, że działania mają sens.

Bezpieczeństwo nie może być oderwane od rzeczywistości firmy - to jej integralna część, nie osobny projekt IT.

Zdarza się jednak, że dostawcy oferują gotowe „pakiety zgodności z CER czy NIS2". Brzmi kusząco...

Kusząco, ale złudnie. Zgodność to nie produkt, który można kupić. CER i NIS2 to ramy, które wskazują cele - a nie gotową receptę. Nie da się ich „zainstalować". Dlatego kiedy słyszę, że dostawca oferuje produkt posiadający certyfikat zgodności z NIS2, zapala mi się czerwona lampka. Zgodność to nie cecha jednego czy drugiego produktu / rozwiązania a cecha efektu jego implementacji w konkretnym środowisku Klienta. W związku z powyższym na ten moment, przykładem realnego certyfikatu do uzyskania lub utrzymania do którego mogą dążyć organizacje to np. certyfikat ISO 27001 - dowód, że organizacja ma działający system zarządzania bezpieczeństwem informacji, nie że kupiła konkretny sprzęt czy oprogramowanie. Dyrektywy wymagają myślenia, a nie odtwórczej implementacji gotowych rozwiązań, nawet takich, które w innych warunkach się sprawdziły i przyniosły zamierzony efekt.

Skoro nie checklisty i gotowe systemy, to od czego zacząć?

Od uczciwej diagnozy - tzw. analizy AS-IS. Trzeba zobaczyć, jak naprawdę wygląda nasza organizacja: jakie procesy i aktywa są kluczowe, na jakie ryzyka są narażone, jak wyglądają aktualne środki zabezpieczeń je chroniące i które z nich faktycznie działają, a które nie. Dopiero potem planujemy stan docelowy, czyli TO-BE - z rozwiązaniami, które mają sens, będą używane i które będą wspierać, a nie przeszkadzać. Nie chodzi o to, by mieć najwięcej funkcjonalności, tylko by systemy wspierały procesy, a nie je paraliżowały.

Czy w tym kontekście kontrola dostępu to wciąż tylko „czytniki i szlabany"?

Cały czas niestety obserwujemy, że z perspektywy wielu organizacji ciągle jeszcze tak, natomiast z perspektywy Vemco, jako odpowiedzialnego dostawcy, zdecydowanie nie. Jednym z ważnych elementów misji, jaką sobie definiujemy w Vemco jest próba zmiany paradygmatu takiego myślenia w organizacjach. Zależy nam na tym, aby organizacje zrozumiały, że przysłowiowy „czytnik" czy „szlaban" sam z siebie nie będzie dobrze wspierał bezpieczeństwa, jeżeli jego typ, miejsce zainstalowania oraz sposób działania nie będą wynikały z kontekstu funkcjonowanie całej organizacji i procesów, które się w niej dzieją. Wydaje mi się, że kluczem do sukcesu jest po prostu zmiana myślenia o kontroli dostępu z modelu funkcjonalno-ilościowego na procesowo-kontekstowy. Takie podejście jest podkreślane przez unijnego ustawodawcę w dyrektywach i takie podejście będziemy starali się propagować jako szansę na wzrost bezpieczeństwa i odporności polskich firm i organizacji.

Czy o rozwiązaniach kontroli dostępu należy myśleć jedynie w kontekście bezpieczeństwa fizycznego?

Absolutnie nie. Kontrola dostępu to narzędzie - strażnik, który sam wymaga ochrony. Z jednej strony broni organizację fizycznie, z drugiej strony stanowi cyber-aktywo, które musi być odporne na cyberzagrożenia.

Oczywiście również jak w poprzednich przypadkach, zgodnie z zasadą adekwatności i proporcjonalności do zidentyfikowanych ryzyk. To przykład, jak przenikają się świat fizyczny i cyfrowy. I to właśnie takie myślenie - z dwóch perspektyw - odróżnia organizacje naprawdę bezpieczne od tych, które tylko wyglądają na bezpieczne.

I właśnie o tych naprawdę bezpiecznych firmach mówi się, że są „odporne". Co właściwie oznacza „odporność organizacji"?

Odporność to zdolność firmy do przetrwania incydentu i powrotu do działania w założonym czasie. To coś więcej niż same procedury - to sposób myślenia. Nie da się całkowicie wykluczyć incydentów - błędów ludzkich, aktów sabotażu czy prób cyberataków - chodzi o to, by potrafić szybko zareagować, minimalizować skutki i wyciągać wnioski na przyszłość. Dlatego odporność wymaga kultury bezpieczeństwa, świadomości i ciągłego doskonalenia - a nie jednorazowego wdrożenia. Bez tego nawet najlepsze technologie nie wystarczą.

Na koniec: jedno zdanie, które chciałbyś, żeby zapamiętali menedżerowie.

Nie da się kupić bezpieczeństwa. Można je tylko budować i pielęgnować – krok po kroku, z głową i w zgodzie z tym, jak naprawdę działa Twoja firma. W Vemco właśnie tak wspieramy naszych klientów: pomagamy ułożyć plan, priorytetyzujemy działania i przeprowadzamy przez ten proces w tempie dostosowanym do budżetu, procesów i możliwości organizacji.

MOBILNE POŚWIADCZENIA – NOWA ERA KONTROLI DOSTĘPU

Kamil Targalski - HID

Rynek systemów kontroli dostępu przechodzi dynamiczną transformację napędzaną cyfryzacją, mobilnością i rosnącymi wymaganiami w zakresie bezpieczeństwa. Jeszcze niedawno standardem były plastikowe karty zbliżeniowe, dziś coraz częściej zastępowane przez poświadczenia mobilne – cyfrowe identyfikatory przechowywane w smartfonach lub smartwatchach. Na tempo tej zmiany znacząco wpływa popularyzacja płatności zbliżeniowych, takich jak Apple Pay i Google Pay.

Mobilne poświadczenia łączą **wygodę, bezpieczeństwo i elastyczność**. Użytkownik nie potrzebuje fizycznej karty – wystarczy urządzenie, które ma zawsze przy sobie. Dostęp odbywa się bezdotykowo, poprzez technologię NFC lub Bluetooth Low Energy (BLE), co zapewnia szybkie i bezpieczne uwierzytelnianie. Takie rozwiązania są szczególnie atrakcyjne w środowiskach korporacyjnych, na uczelniach i w budynkach użyteczności publicznej, gdzie płynne, intuicyjne doświadczenie użytkownika staje się wyznacznikiem innowacyjności oraz atrakcyjności miejsca pracy lub samego budynku.

Migracja z tradycyjnych kart do rozwiązań mobilnych to naturalny krok w kierunku integracji i cyfryzacji procesów bezpieczeństwa. Mobilny dostęp nie tylko podnosi komfort użytkowników, ale także znacząco ułatwia **zarządzanie cyklem życia poświadczeń** – ich wydawanie, cofanie czy modyfikację można realizować zdalnie, bez drukowania i dystrybucji kart. To nie tylko oszczędność czasu i kosztów, lecz również ograniczenie zużycia plastiku i odpadów. Odchodzą również koszty związane z personalizacją kart takie jak zakup, utrzymanie oraz serwis drukarek i materiałów eksploatacyjnych.

Kolejnym atutem poświadczeń mobilnych jest ich **wyższy poziom bezpieczeństwa**. W przeciwieństwie do kart zbliżeniowych opartych na starszych technologiach,

(np. 125 kHz) lub kart 13.56 MHz z przestarzałymi metodami szyfrowania, które łatwo sklonować - cyfrowe identyfikatory korzystają z zaawansowanego szyfrowania oraz pozwalaja wymusić na użytkowniku dodatkowe uwierzytelnienie w postaci PIN'u, odcisku palca lub rozpoznawania twarzy. Uzyskujemy wtedy system kontroli dostępu w modelu **Multi-Factor-Authentication by default** przy wykorzystaniu prostszych oraz tańszych czytkniów bez klawiatury lub biometryki. Urządzenie mobilne może przechowywać wiele poświadczeń równolegle – nie tylko do drzwi, lecz także do komputerów, drukarek czy aplikacji firmowych.

Nowym etapem rozwoju są poświadczenia przechowywane w **Apple Wallet** i **Google Wallet**. Dane użytkownika zabezpieczone są w sprzętowo izolowanym module Secure Element, tym samym, który chroni karty płatnicze. Każda interakcja jest szyfrowana i chroniona biometrią. Dostęp realizowany jest natychmiast – wystarczy zbliżyć telefon do czytnika NFC, bez konieczności otwierania aplikacji czy aktywowania połączenia Bluetooth. W porównaniu z rozwiązaniami BLE, które często wymagają uruchomienia aplikacji i nawiązania połączenia, Wallet zapewnia większą niezawodność i prostotę obsługi.

Wdrażanie mobilnych rozwiązań wiąże się jednak z koniecznością modernizacji infrastruktury. **Czytniki muszą obsługiwać protokoły NFC lub BLE**, na szczęście większość czytników HID sprzedanych na przestrzeni lat 2018-2025 wspiera jeden lub oba z nich.

W przypadku konieczności modernizacji systemu oraz wymiany czytników, organizacje coraz częściej wybierają otwarte standardy komunikacyjne takie jak **OSDP (Open Supervised Device Protocol** rekomendowany w normie systemów alarmowych EN60839), które zapewniają kompatybilność z różnymi dostawcami i umożliwiają dalszy rozwój technologiczny bez uzależnienia od jednego producenta.

Rosnące znaczenie mają także aspekty zrównoważonego rozwoju. Rezygnacja z plastikowych kart i centralne zarządzanie poświadczeniami przyczyniają się do zmniejszenia śladu węglowego, co wpisuje się w politykę ESG coraz większej liczby firm. W tym kontekście technologia mobilna staje się nie tylko bardziej nowoczesna, ale również bardziej odpowiedzialna.

Transformacja w kierunku mobilnych poświadczeń jest więc nieunikniona. Choć wiele organizacji wciąż wykorzystuje tradycyjne karty, coraz więcej z nich przygotowuje się do pełnej cyfryzacji dostępu. Trend ten wspierany jest przez rozwój infrastruktury mobilnej, popularyzacji płatności zbliżeniowych Apple Pay oraz Google Pay, wzrost świadomości bezpieczeństwa oraz potrzebę tworzenia bardziej inteligentnych i elastycznych środowisk pracy. W rezultacie smartfon – dotychczas narzędzie komunikacji – staje się również kluczem do budynku, biura czy przestrzeni współdzielonej.

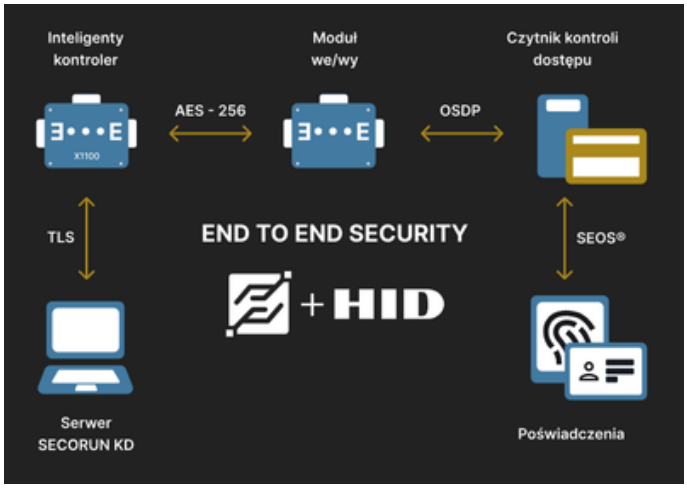
SECORUN x HID - END TO END SECURITY W PRAKTYCE

Maciej Boguniecki - Vemco

Bezpieczeństwo systemów kontroli dostępu wymaga dziś nie tylko sprawnej integracji technologicznej, lecz także pełnej spójności komunikacji między wszystkimi elementami systemu – od poświadczenia użytkownika po warstwę serwerową.
Rozwiązanie SECORUN w połączeniu z kontrolerami HID Aero zostało zaprojektowane w architekturze **End-to-End Security**, której celem jest ochrona całego łańcucha autoryzacji.

Bezpieczeństwo jako integralna architektura

System pracuje w oparciu o pełne szyfrowanie komunikacji na każdym etapie wymiany danych.
Poświadczenia użytkownika chronione są już w momencie ich użycia – między kartą lub Mobile ID a czytnikiem – dzięki technologii **HID Seos®**, wykorzystującej unikalne klucze kryptograficzne dla każdej sesji.



Dalej, komunikacja pomiędzy czytnikiem a modułami I/O odbywa się poprzez **OSDP** (Open Supervised Device Protocol) w wersji 2.2, co uniemożliwia ingerencję w przewody transmisyjne czy próby przechwycenia sygnału.
Dane przesyłane z portów I/O do kontrolera HID Aero szyfrowane są w standardzie AES-256, a transmisja między kontrolerem a oprogramowaniem SECORUN KD wykorzystuje protokół TLS 1.3 w środowisku zgodnym z FIPS 140-2.
Takie podejście eliminuje typowe punkty podatności - np. niezabezpieczone linie danych lub brak integralności sygnału - i gwarantuje, że żaden z elementów infrastruktury nie może zostać użyty jako wektor ataku.

Zasada spójnego łańcucha autoryzacji

W architekturze End-to-End Security każdy etap komunikacji w systemie stanowi część kontrolowanego, kryptograficznie zabezpieczonego procesu:

- Poświadczenie → Czytnik: autoryzacja i szyfrowanie HID Seos®.
- Czytnik → Kontroler: komunikacja szyfrowanym protokołem OSDP v2.
- Kontroler → Host: szyfrowanie danych AES-256 i uwierzytelnianie TLS/FIPS.

Taka struktura **pozwala zachować integralność systemu** nawet w przypadku fizycznego naruszenia pojedynczego elementu.

SECORUN MOBILE ID – DOSTĘP W PORTFELU, BEZPIECZEŃSTWO W ARCHITEKTURZE

NEW

Maciej Boguniecki - Vemco

Nowym elementem ekosystemu SECORUN jest rozwiązanie **SECORUN Mobile ID**, które umożliwia przechowywanie cyfrowych poświadczeń dostępowych w portfelach mobilnych **Apple Wallet** i **Google Wallet**.
To rozszerzenie architektury bezpieczeństwa o warstwę mobilną, zachowujące pełną zgodność z zasadami **End-to-End Security.**
Rezultatem jest połączenie systemu SECORUN z **globalnymi ekosystemami mobilnych portfeli**.

Jak to działa?

Integracja SECORUN z platformą HID Mobile Access umożliwia wydawanie i zarządzanie poświadczeniami wirtualnymi bez potrzeby stosowania kart fizycznych.
System pozwala administratorom **zdalnie przydzielać, modyfikować i odbierać cyfrowe karty dostępu** w czasie rzeczywistym - bez konieczności kontaktu z użytkownikiem.
Nowe poświadczenia są aktywowane w urządzeniu mobilnym, a ich cofnięcie skutkuje natychmiastowym zablokowaniem dostępu.

Identyfikatory Mobile ID przechowywane są w **Secure Element** urządzenia mobilnego – wydzielonym układzie kryptograficznym, do którego nie ma dostępu ani system operacyjny, ani inne aplikacje. Proces autoryzacji odbywa się z wykorzystaniem biometrii (**Face ID / Touch ID**) oraz lokalnej weryfikacji klucza prywatnego przypisanego do tożsamości użytkownika.
W praktyce oznacza to, że nawet w przypadku utraty telefonu poświadczenie **nie może zostać skopiowane**, wyeksportowane ani użyte bez zgody właściciela.

To poziom bezpieczeństwa i elastyczności zarządzania, którego żadne fizyczne karty nie są w stanie zapewnić.

Mobilny dostęp z rozszerzoną funkcjonalnością

Aplikacja SECORUN Mobile ID została zaprojektowana nie tylko jako klucz dostępu, ale również jako **narzędzie zarządzania i komunikacji w organizacji.**

Pozwala na:

- bezpieczne logowanie użytkowników i autoryzację wejść,
- zarządzanie kartami Mobile ID **bezpośrednio z poziomu systemu SECORUN Kontrola Dostępu,**
- wysyłanie komunikatów alarmowych, ogłoszeń pracowniczych oraz powiadomień systemowych do wybranych grup użytkowników.

Dzięki temu bezpieczeństwo staje się **aktywnym kanałem interakcji** pomiędzy użytkownikiem a organizacją, a nie odrębnym modułem IT.
Aplikacja SECORUN Mobile ID jest dostępna w **sklepach App Store i Google Play**, co pozwala użytkownikom szybko i bezpiecznie aktywować cyfrowe poświadczenia dostępu w środowisku zgodnym z globalnymi standardami bezpieczeństwa.

Download on the App Store

GET IT ON Google Play

Vemco Summit 2025 dobiegł końca, ale rozmowa o bezpieczeństwie trwa dalej.

Dziękujemy za zaufanie, inspirujące dyskusje i otwartość, która napędza nas do działania.
Zapraszamy do kontaktu, współpracy i wspólnego budowania ekosystemu bezpieczeństwa - mądrego, spójnego i gotowego na przyszłość.