ul. Rakowiecka 36, 02-532 Warszawa, tel. +48 22 646-68-73; fax +48 22 606-37-80, e-mail: sales@cc.com.pl

http://www.cc.com.pl/

CC - Integrator systemów sieciowych i bezpieczeństwa

„Realizujemy projekty infrastruktury i bezpieczeństwa sieciowego”.

- CC Otwarte Systemy Komputerowe Sp. z o.o. - spółka prywatna założona w 2001.
- Od 2001 r. skupiamy się na trzech kluczowych obszarach IT: sieciach, bezpieczeństwie i tworzeniu oprogramowania.
- Dostarczamy komplet rozwiązań i usług tworzących efektywne, bezpieczne i niezawodne środowisko IT.

ul. Rakowiecka 36, 02-532 Warszawa, tel. +48 22 646-68-73; fax +48 22 606-37-80, e-mail: sales@cc.com.pl

Co oferujemy?

Dostawy rozwiązań IT z obszarów: bezpieczeństwa, sieci, sprzętu i oprogramowania.

- Firewall i bezpieczeństwo
- Sieci LAN i WAN
- Systemy Wi-Fi
- Systemy autoryzacji dwuskładnikowej - 2FA
- Systemy monitorowania, kontroli dostępu i zarządzania sieciami
- Ochrona endpoint i systemy DLP

- Usługi wdrożeniowe i wsparcie techniczne
- Szkolenia i warsztaty
- Inne usługi profesjonalne: projekty, audyty, ekspertyzy

Firewall i bezpieczeństwo

Właściwa ochrona systemów IT wymaga, aby zabezpieczenia były dostosowane do zmian w architekturze sieci oraz do nowych zagrożeń. Tradycyjne systemy zabezpieczeń, które spełniały wszystkie oczekiwania i zapewniały bezpieczeństwo kilka lat temu, są obecnie nieadekwatne zarówno pod względem rosnących potrzeb funkcjonalnych, jak i zapewnianego poziomu ochrony. Standardy bezpieczeństwa obowiązujące jeszcze 3 - 4 lata temu, tj.: system firewall filtrujący ruch na podstawie portu sieciowego i adresu oraz system antywirusowy usuwający złośliwy kod, w dobie zagrożeń takich jak ataki "zero-day" oraz "APT" stają się zdecydowanie przestarzałe.

Ochrona przed współczesnymi zagrożeniami

- Ochrona sieci i użytkowników przed złośliwym oprogramowaniem typu: ransomware, boty, APT, wirusy i inne.
- Pełna inspekcja danych dla różnych protokołów sieciowych (funkcje AV/IDS/IDP).
- Filtracja danych dla różnorodnych aplikacji WWW - np. Facebook, komunikatory, systemy webmail.
- Limitowanie przepustowości, np.: Facebook, YT.

Wysoka wydajność

- Wymagania względem wydajności współczesnych systemów bezpieczeństwa rosną z powodu wzrostu przepustowości łącz internetowych oraz zwiększenia wydajności LAN.
- Konieczności filtrowania nie tylko nagłówków, ale i całej zawartości pakietów odbija się na wydajności.
- Funkcje deszyfracji ruchu także wymagają wydajnych platform.
- Oferowane przez nas systemy zapewniają pełną filtrację przepustowości od 0,5 Gbps, poprzez systemy średniej skali: 1 Gbps do 10 Gbps, do systemów o przepustowości powyżej 10 Gbps aż do 200 Gbps.

Centrum danych, chmura prywatna i publiczna

- Rozwiązania, które oferujemy pozwalają na pełną integrację z platformami wirtualizacyjnymi, takimi jak np.: VMware, VMware NSX, Hyper-V, VirtualBox i innymi.
- Oferujemy też systemy funkcjonujące w chmurze publicznej, a także chroniące platformy i oprogramowanie dostępne w chmurze publicznej.

Oferujemy:

- Dostawy oprogramowania, sprzętu, wsparcia i subskrybcji.
- Usługi: analiza potrzeb, projekty, testy i diagnostyka istniejącej infrastruktury, częściowe lub pełne migracje, wdrażania i konfiguracja dostarczonego sprzętu, nadzór oraz utrzymanie w trybie 24x7, szkolenia warsztatowe.

REFERENCJE:

- Najwyższa Izba Kontroli,
- Urząd Transportu Kolejowego,
- MPWiK w Warszawie,
- banki i instytucje finansowe,
- wiodąca firma doradcza.

paloalto NETWORKS

Check Point

FORTINET

JUNIPER NETWORKS

FIREMON

FORCEPOINT powered by Raytheon

ul. Rakowiecka 36, 02-532 Warszawa, tel. +48 22 646-68-73; fax +48 22 606-37-80, e-mail: sales@cc.com.pl

http://www.cc.com.pl/

Sieci LAN i WAN

Sprawnie i wydajnie działająca sieć lokalna jest niezbędnym elementem infrastruktury każdej firmy. Rosnące zapotrzebowanie na dane, wynikające zarówno z potrzeb współczesnych aplikacji, jak i ze zwiększenia liczby urządzeń korzystających z sieci, powoduje wzrost oczekiwań co do możliwości sieci lokalnej. Współczesna sieć musi też podołać takim wyzwaniom jak: przesył danych multimedialnych, wirtualizacja serwerów, dostęp do chmury publicznej i prywatnej, backup on-line.

Wysoka wydajność i elastyczność konfiguracji

- Oferujemy przełączniki oraz rutery z portami o przepustowości: 1 Gbps, 2,5 Gbps, 10 Gbps, 25 Gbps, 40 Gbps, 100 Gbps oraz 400 Gbps.
- Technologie Ethernet 10/25/40 Gbps jeszcze niedawno uznawane za bardzo kosztowne i zarezerwowane wyłącznie do zaawansowanych rozwiązań DataCenter są obecnie dostępne w niewygórowanych cenach.
- Przełączniki PoE pozwalające na zasilanie punktów dostępowych WiFi oraz telefonów IP.
- Elastyczna konfiguracja: wirtualne stosy, agregacja portów, konfiguracje kandydackie, obsługa technologii SDN (Software Defined Networking) oraz wirtualizacji (VxLAN).
- Oferujemy też rozwiązania monitoringu sieci.

Niezawodność

- Oferowane przez nas rozwiązania posiadają dożywotnią gwarancję i wsparcie producenta z opcją wymiany w trybie co najmniej "next-day".
- Możliwe jest uruchomienie konfiguracji redundantnych, w których awaria jednego z komponentów nie powoduje przestoju w pracy systemu.
- Oferujemy pełen zakres usług serwisowych.

Bezpieczeństwo

- Wielowarstwowe bezpieczeństwo danych.
- Odseparowanie ruchu pochodzącego z różnych: działów, źródeł, sieci logicznych.
- Technologia 802.1x pozwalająca na zablokowanie dostępu do sieci niezautoryzowanych urządzeń i użytkowników.

Oferujemy:

- Dostawy sprzętu.
- Usługi: analiza potrzeb, projekty, testy i diagnostyka istniejącej infrastruktury, częściowe lub pełne migracje, wdrażania i konfiguracja dostarczonego sprzętu, nadzór oraz utrzymanie w trybie 24x7, szkolenia warsztatowe.

REFERENCJE:

- Krajowe Biuro Wyborcze,
- Urząd Transportu Kolejowego,
- Instytut Podstaw Informatyki PAN,
- wiodące kancelarie prawne,
- banki i instytucje finansowe.

RUCKUS

JUNIPER NETWORKS

ARISTA

aruba a Hewlett Packard Enterprise company

CISCO

GBC PHOTONICS DRIVING OPTICAL NETWORKS

A10 Networks

radware Every second counts

ul. Rakowiecka 36, 02-532 Warszawa, tel. +48 22 646-68-73; fax +48 22 606-37-80, e-mail: sales@cc.com.pl

http://www.cc.com.pl/

Systemy Wi-Fi

Oferujemy systemy sieci bezprzewodowych Wi-Fi dostosowane do potrzeb różnorodnych użytkowników - środowisk biurowych, logistyki i transportu, edukacji, przemysłu, placówek medycznych obiektów sportowych i innych.

Wysoka przepustowość i pełne pokrycie obiektu siecią

- Systemy pracujące w pasmach 2,4 oraz 5 Ghz pozwalają na osiągnięcie przepustowości do 1733 Mbit/s i obsługę do 512 użytkowników przez jeden punkt dostępowy.
- Zaawansowane techniki radiowe pozwalają na dwukrotne zmniejszenie liczby punktów dostępowych niezbędnych do pokrycia obiektu siecią.
- Rozwiązania wykorzystujące kontroler (sprzętowy, programowy, chmurowy lub rozproszony) pozwalają na zarządzanie siecią liczącą od kilku do nawet tysięcy AP.

Niezawodność

- Dożywotnia gwarancja i wsparcie producenta z opcją wymiany w trybie "next-day".
- Możliwe jest uruchomienie konfiguracji redundantnych, w których awaria kontrolera nie powoduje przestoju w pracy systemu.

Systemy do zadań specjalnych

- AP o podwyższonej odporności na czynniki środowiskowe.
- AP przemysłowe, specjalne rozwiązania dla środków transportu, stadionów i obiektów sportowych oraz radiolinie.

Bezpieczeństwo

- Separacja dostępu dla pracowników i gości oraz ruchu sieciowego użytkowników autoryzowanych i anonimowych.
- Zintegrowanie systemu kont użytkowników z domeną Windows lub wprowadzenie niezależnego systemu weryfikacji tożsamości.
- System jednorazowych "biletów" do Wi-Fi, ważnych przez określony czas.

REFERENCJE:

- Urząd Transportu Kolejowego,
- MPWiK w Warszawie,
- Instytut Gruźlicy i chorób Płuc,
- Uczelnia Vistula,
- hotele, banki i instytucje finansowe,
- urzędy miast, powiatów i gmin,
- szkoły i instytucje edukacyjne.

RUCKUS

aruba
a Hewlett Packard Enterprise company

AEROHIVE NETWORKS

Extreme networks

JUNIPER NETWORKS

ul. Rakowiecka 36, 02-532 Warszawa, tel. +48 22 646-68-73; fax +48 22 606-37-80, e-mail: sales@cc.com.pl

http://www.cc.com.pl/

Autoryzacja

Autoryzacja dostępu do systemów i aplikacji jest podstawowym ogniwem bezpieczeństwa informatycznego. Bez niezawodnej i bezpiecznej weryfikacji tożsamości: klienta, użytkownika i administratora nie jest możliwe zapewnienie bezpieczeństwa infrastruktury IT. Autoryzacja obejmuje dostęp do takich systemów jak: komputery desktop, serwery (w trybie administratora), zdalne pulpity, aplikacje chmurowe, sieci VPN, itd. Statyczne hasła dla użytkownika odchodzą do przeszłości. Autoryzacja dostępu bazująca na dodatkowym czynniku uwierzytelniającym (2FA - two factor authentication) jest wymagana w niektórych branżach (np. usług finansowych), a zalecana w praktycznie każdym obszarze IT.

Autoryzacja OTP

- Wykorzystanie sprzętowego lub programowego generatora haseł jednorazowych.
- Każda operacja wymagająca autoryzacji musi być uwierzytelniona poprzez OTP.
- Wymaga serwera autoryzacji.

Autoryzacja PKI

- Bazuje na standardach kryptografii asymetrycznej (tj. z kluczem prywatnym i publicznym).
- Token (lub karta) sprzętowy w bezpieczny sposób przechowuje klucz prywatny użytkownika, który jest fizycznie zabezpieczony przed nielegalnym skopiowaniem z tokena.
- Bazuje na cyfrowych certyfikatach w formacie x509v3.
- Wykorzystywane jest m.in. w autoryzacji VPN a także dostępu do: sieci w standardzie 802.1x, serwisów WWW, stanowisk desktop i innych.

Oferowane przez nas rozwiązania autoryzacyjne

- Tokeny sprzętowe: “kalkulator” (pinpad) - z wyświetlaczem i klawiaturką numeryczną, “breloczek” - z samym wyświetlaczem, "Cronto" - z kamerką i wyświetlaczem rozpoznające kolorowe kody 2D, zintegrowanym czytnikiem kart EMV.
- PKI: tokeny w postaci USB-dongle oraz karty mikroprocesorowe (SC), hybrydowe - OTP / PKI.
- Rozwiązania softwarowe: tokeny na smartfony, autoryzacja SMS.

REFERENCJE:

- Firma ubezpieczeniowa,
- banki i instytucje finansowe,
- firmy z sektora High-Tech.

THALES

HID

VASCO
TRUST FOR THE DIGITAL WORLD

OneSpan
Be bold. Be secure.

NACVIEW

ul. Rakowiecka 36, 02-532 Warszawa, tel. +48 22 646-68-73; fax +48 22 606-37-80, e-mail: sales@cc.com.pl

Monitoring, kontrola dostępu, zarządzanie

Współczesne sieci wymagają dodatkowych rozwiązań, będących uzupełnieniem podstawowych funkcji bezpieczeństwa zapewnianych przez firewall-e. Funkcjonalności takie oferują między innymi systemy monitorowania zdarzeń i przepływów sieciowych, systemy zdalnego dostępu oraz systemy monitorowania sesji i zarządzające dostępem.

Systemy monitorowania zdarzeń i przepływów sieciowych

- System monitorowania wykrywa i reaguje na zagrożenia, takie jak: ataki DDoS, infekcje mallware, awarie sprzętu, wadliwe aplikacje i złośliwe działanie użytkowników.
- Systemy monitorowania przepływów pozwalają na poznanie w czasie rzeczywistym charakterystyki ruchu w sieci, wykrywanie i diagnostykę problemów związanych z wydajnością i bezpieczeństwem LAN i WAN.
- NBA - moduł analizatora zachowania (Network Behavior Analysis) pozwala na wyizolowanie konkretnych dozwolonych, zakazanych lub podejrzanych wzorców komunikacji.

Systemy NAC (Network Access Control)

- Kontrola dostępu - bez odpowiedniej autoryzacji użytkownik lub urządzenie nie otrzyma fizycznego dostępu do sieci lub uzyska ograniczony dostęp.
- NAC realizuje politykę AAA (Authorization, Authentication and Accounting) w odniesieniu do wszystkich użytkowników i urządzeń.
- Protokoły takie jak 802.1X zapewniają bezpieczeństwo poprzez szyfrowanie transmisji danych.

Systemy zdalnego dostępu

- Pozwalają na zrealizowanie bezpiecznego dostępu do: wybranych serwisów, zasobów i aplikacji dla użytkowników zewnętrznych.
- Nie wymagają instalacji dedykowanego klienta VPN (lub też instalacja ta jest niezwykle uproszczona).
- Zakres dostępu może obejmować: wewnętrzne aplikacje WWW, pocztę elektroniczną, serwery plików, aplikacji Windows, a nawet dostęp do pulpitu wybranych komputerów.

Systemy monitorowania sesji

- Pozwalają na pełną kontrolę sesji realizowanych zarówno wewnątrz sieci LAN jak i sesji zdalnych (inicjowanych z Internetu)
- Kontrola obejmuje takie protokoły jak np.: SSH, RDP, telnet, X11, HTTP/HTTPS.
- Realizowany jest nadzór oraz nagrywanie sesji zarówno tekstowych (np. SSH) jak i graficznych (RDP).
- Mogą też pełnić rolę pośrednika przy autoryzacji użytkowników, dzięki czemu zewnętrzni dostawcy nie muszą posiadać bezpośrednich poświadczeń bezpieczeństwa do naszych systemów.
- Znajdują zastosowanie w monitoringu działań zewnętrznych dostawców usług a także przy kontroli działania użytkowników uprzywilejowanych (administratorów, operatorów, itp.).

REFERENCJE:

- Giełda Papierów Wartościowych S.A. w Warszawie,
- Krajowe Biuro Wyborcze,
- Najwyższa Izba Kontroli,
- banki i instytucje finansowe.

Flowmon Driving Network Visibility

FORESCOUT

FUDO SECURITY

NACVIEW

Nagios®

SECUREVISIO

Pulse Secure®

splunk>

ul. Rakowiecka 36, 02-532 Warszawa, tel. +48 22 646-68-73; fax +48 22 606-37-80, e-mail: sales@cc.com.pl

http://www.cc.com.pl/

Ochrona endpoint i DLP

Pomimo powszechnej dostępności produktów zapewniających bezpieczeństwo, np. systemów antywirusowych, systemy komputerowe są infekowane w zastraszającym tempie nowym rodzajami złośliwego oprogramowania. Ataki przybierają różne formy i pojawiają się korzystając z różnych dróg, np. poprzez zarażone strony WWW, pocztę elektroniczną lub zewnętrzne pamięci USB. Tradycyjne metody ochrony nie są w stanie nadążać za gwałtownie zmieniającym się krajobrazem zagrożeń.

Zabezpieczenie platform endpoint

- Przez platformy "endpoint" ("końcówki") - komputery PC - stacjonarne i notebooki.
- Tradycyjną formą ochrony endpoint jest coraz mniej skuteczny antywirus oraz lokalny firewall.
- Rozwiązanie AV bazujące ma porównaniu pliku z bazą wzorców mogą być uzupełnieniem mechanizmów ochrony, lecz nie jedynym zabezpieczeniem.
- Współczesne oprogramowanie zabezpieczające, działając na poziomie systemu operacyjnego wykrywa wzorce zachowań typowe dla złośliwego oprogramowania i w przypadku skumulowania podejrzanych sekwencji czynności blokuje wykonanie programu.

Rozwiązania pokrewne - szyfrowanie

- Zabezpieczenia zasobów dyskowych notebooków, stacji roboczych i serwerów poprzez szyfrowanie.
- Zabezpieczenie dokumentów elektronicznych i poczty elektronicznej poprzez podpisy elektroniczne i szyfrowanie.

Zabezpieczenie platform mobilnych

- Prywatne smartfony i tablety są powszechnie wykorzystywane w sieciach korporacyjnych .
- BYOD (Bring Your Own Device) to nowe zagrożenia związane z wprowadzeniem do sieci urządzeń, na którymi organizacja nie sprawuje kontroli: zainfekowany smartfon może okazać się równie niebezpieczny jak zarażony wirusem komputer PC.
- Izolowanie oraz kontrolę urządzeń mobilnych zapewnia oprogramowanie typu "Mobile Endpoint Security" oraz EMM (Enterprise Mobility Management).

REFERENCJE:

- Krajowe Biuro Wyborcze,
- jednostki samorządu terytorialnego,
- banki i instytucje finansowe,
- wiodące kancelarie prawne,
- firmy produkcyjne.

Check Point
COSOSYS
FUDO SECURITY
FORCEPOINT
paloalto NETWORKS
SOPHOS
TREND MICRO

ul. Rakowiecka 36, 02-532 Warszawa, tel. +48 22 646-68-73; fax +48 22 606-37-80, e-mail: sales@cc.com.pl
http://www.cc.com.pl/

CC w liczbach

- **2** certyfikaty CISSP ISC2
- **7** kluczowych partnerów technologicznych
- **15** mln złotych obrotów w 2018 r.
- **18** lat doświadczenia w tworzeniu systemów bezpieczeństwa
- **30** przeprowadzonych szkoleń własnych*
- **30** (ponad) producentów rozwiązań IT w ofercie
- **40** aktualnych certyfikatów inżynierskich z 10 specjalizacji
- **200** przeszkolonych klientów*
- **250** (ponad) wdrożonych systemów bezpieczeństwa*
- **500** (ponad) dostarczonych systemów bezpieczeństwa*

(*) od stycznia 2016 roku do stycznia 2019 roku.

ul. Rakowiecka 36, 02-532 Warszawa, tel. +48 22 646-68-73; fax +48 22 606-37-80, e-mail: sales@cc.com.pl
http://www.cc.com.pl/

Wdrożenia i wsparcie

Wspieramy wszystkie oferowane przez nas rozwiązania.

Oferujemy nie tylko dostawy sprzętu i oprogramowania ale także pełną gamę usług: prowadzimy analizę potrzeb klientów, projektujemy systemy bezpieczeństwa oraz integrujemy je z systemami zdalnego dostępu, infrastrukturą VPN, systemem domenowym, itd. Realizujemy testy oraz diagnostykę istniejącej infrastruktury, wykonujemy częściowe lub pełne migracje rozwiązań sieciowych, prowadzimy nadzór oraz utrzymanie w trybie 24x7, a także realizujemy szkolenia warsztatowe.
Wszystkie usługi wykonywane są przez naszych pracowników posiadających certyfikaty inżynierów danego producenta - posiadamy i utrzymujemy aktualne certyfikacje wszystkich kluczowych, znajdujących się w naszej ofercie producentów.

Oferujemy usługi:

- projektowe,
- wdrożeniowe,
- wsparcia gwarancyjnego i pogwarancyjnego.

Wsparcie:

- Poziom wsparcia dostosowujemy do potrzeb klienta: 24x7, 8x5, ...
- Realizujemy zdalny nadzór i monitoring infrastruktury klientów.

ul. Rakowiecka 36, 02-532 Warszawa, tel. +48 22 646-68-73; fax +48 22 606-37-80, e-mail: sales@cc.com.pl
http://www.cc.com.pl/

Szkolenia, warsztaty, seminaria

Realizujemy

- Realizujemy szkolenia autorskie i szkolenia warsztatowe.

Dysponujemy

- Dysponujemy klimatyzowanymi salami szkoleniowymi.

Oferujemy

- Oferujemy szkolenia autoryzowane wybranych producentów (poprzez partnerskie ATC).
- Oferujemy szkolenia u klienta, realizowane na sprzęcie własnym lub klienta.

ul. Rakowiecka 36, 02-532 Warszawa, tel. +48 22 646-68-73; fax +48 22 606-37-80, e-mail: sales@cc.com.pl

http://www.cc.com.pl/

Inne usługi

- Projektowanie sieci i systemów.
- Automatyzacja i orkiestracja systemów bezpieczeństwa – tworzenie skryptów, integracja poprzez API.
- Projektowanie, analiza i audyt sieci Wi-Fi, w tym usługi pre- i post-installation Site-Survey.
- Audyty: bezpieczeństwa infrastruktury i aplikacji, audyty GDPR/RODO, inne - specjalizowane.

Tworzenie oprogramowania na zamówienie

- Oprogramowanie biznesowe
  - specjalizujemy się w obsłudze nietypowych usług i procesów.
- Automatyzacja i orkiestracja systemów bezpieczeństwa.
- Aplikacje mobilne i aplikacje dla IoT.
- Technologie: Microsoft/.Net; C/C++; Python.

REFERENCJE:

Firmy ubezpieczeniowe,

Firmy z sektora bankowo-finansowego,

Operatorzy telekomunikacyjni i dostawcy usług,

Instytucje naukowe.

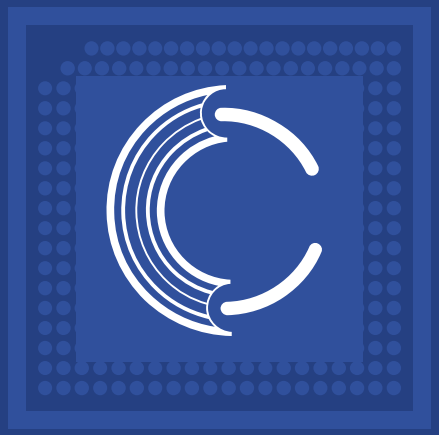
ul. Rakowiecka 36, 02-532 Warszawa, tel. +48 22 646-68-73; fax +48 22 606-37-80, e-mail: sales@cc.com.pl

http://www.cc.com.pl/

Partnerzy technologiczni

ul. Rakowiecka 36, 02-532 Warszawa, tel. +48 22 646-68-73; fax +48 22 606-37-80, e-mail: sales@cc.com.pl

http://www.cc.com.pl/



CC Otwarte Systemy Komputerowe

Więcej informacji znajdziecie Państwo
w Internecie, na stronach:
http://www.cc.com.pl/
http://www.wifi.com.pl/

Kontakt:
Kontakt ogólny: cc@cc.com.pl
Dział Handlowy: sales@cc.com.pl
Dział Techniczny: tech@cc.com.pl

ul. Rakowiecka 36, 02-532 Warszawa
tel. +48 22 646-68-73; fax +48 22 606-37-80
e-mail: sales@cc.com.pl