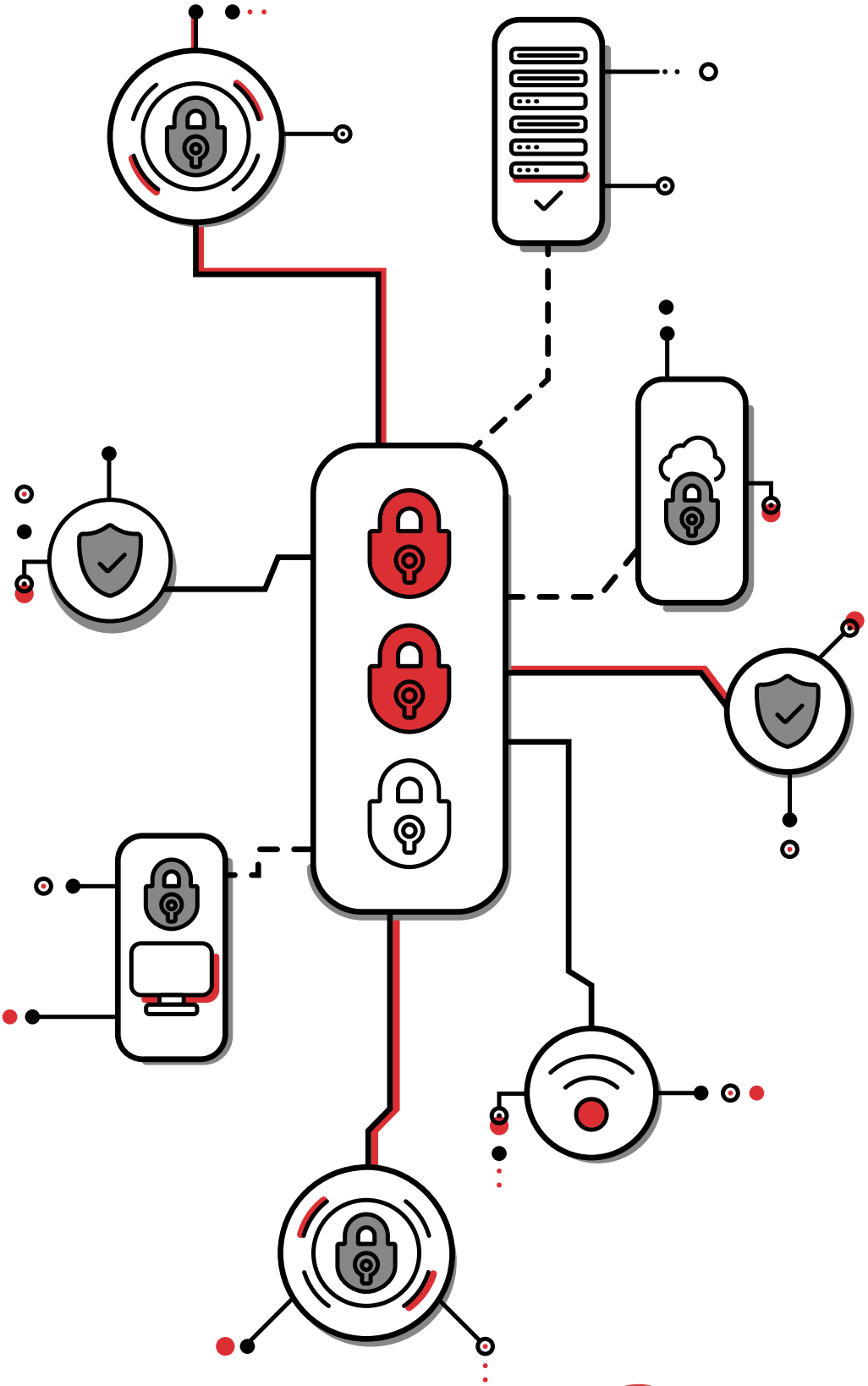

Sprint

CYBERSECURITY

Dla zapewnienia poufności i integralności Państwa danych oraz ochrony przed próbami nieuprawnionej ingerencji w system, dostarczamy kompleksowe rozwiązania bazujące na różnorodnych technologiach i narzędziach renomowanych dostawców.

Posiadamy certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001, wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób.

Poznaj nasze usługi

NETWORK / CLOUD SECURITY

Od kilku lat zachodzą poważne zmiany w charakterystyce ruchu WAN i użytkownicy sieci coraz częściej korzystają z usług zlokalizowanych w różnych obszarach sieci WAN, w tym w chmurze, a generowany przez nich ruch oparty jest na konsumpcji aplikacji. Organizacja wydajnej, niezawodnej i co bardzo ważne – bezpiecznej infrastruktury sieciowej WAN do obsługi wymagających aplikacji biznesowych jest niezwykle trudnym wyzwaniem, który potrzebuje zastosowania różnych technologii.

SD-WAN

To podejście do sieci definiowanej programowo (SDN), które przenosi zarządzanie ruchem sieciowym z dala od sprzętu do warstwy aplikacji. SD-WAN, zapewnia możliwość zdefiniowania kategorii ruchu i obowiązującej logiki kierowania określonego typy ruchu mniej obciążonym łączem.

CASB

To natywna dla chmury usługa subskrypcji Cloud Access Security Broker (CASB), która została zaprojektowana w celu zapewnienia widoczności, zgodności, bezpieczeństwa danych i ochrony przed zagrożeniami dla usług opartych na chmurze.

SASE

To koncepcja sieciowej architektury, która łączy technologię sterowanej programowo sieci rozległej SD-WAN z mechanizmami bezpieczeństwa, tworząc łatwą do wdrożenia usługę chmurową.

PERIMETER SECURITY

Konieczność zabezpieczenia granic naszej sieci jest dość oczywista. Sam wybór technologii, które zapewniają różny poziom zabezpieczenia innych typów zasobów jest już zagadnieniem mniej oczywistym.

NEXT GENERATION FIREWALL

Zapewnia ochronę przed zagrożeniami wewnętrznymi i zewnętrznymi poprzez identyfikację oraz możliwość blokowania ataków czy złośliwego oprogramowania. Nowoczesne Firewall'e zapewniają ponadto wiele dodatkowych mechanizmów bezpieczeństwa, w tym w szczególności:

- OCHRONĘ ANTYWIRUSOWĄ
- FILTROWANIE URL
- OCHRONĘ IPS
- KONCENTRACJĘ VPN
- KONTROLĘ APLIKACJI
- OCHRONĘ OT
- KONTROLĘ ZGODNOŚCI Z REGULACJAMI

WEB APPLICATION FIREWALL

To specjalizowane rozwiązanie dedykowane do ochrony aplikacji webowych, opartych na komunikacji za pomocą protokołu http/https, które w szczególności zapewnia:

- OCHRONĘ PRZED ATAKAMI WIELOWEKTOROWYMI
- ANTY-DDOS
- ANALIZĘ HEHAWIORALNĄ W OPARCIU O AI
- SSL OFFLOAD
- PREDEFINIOWANE PROFILE BEZPIECZEŃSTWA
- MOŻLIWOŚĆ REALIZACJI RÓŻNORODNYCH SCENARIUSZY WDROŻENIOWYCH

SECURE EMAIL GATEWAY

To zaawansowana, wielowarstwowa ochrona przed pełnym spektrum zagrożeń przenoszonych przez pocztę e-mail – spam, phishing, złośliwe oprogramowanie, zagrożenia 0-day, podszywanie się.

AUTHENTICATION AND ACCESS CONTROL

To bezpieczne i efektywne zarządzanie tożsamością cyfrową poprzez właściwe procesy uwierzytelniania i autoryzacji użytkowników zgodnie z zasadą Zero Trust Access.
Dla zapewnienia kontroli i bezpieczeństwa cyfrowej tożsamości wdrażamy szereg mechanizmów i technologii, w tym między innymi:

- **NAC – Network Access Control** zapewnia pełną widoczność urządzeń, w tym urządzeń IoT w sieciach korporacyjnych. Dzięki niemu zespoły IT mogą łatwo rozpoznać kto i do czego uzyskuje dostęp w sieci, a także jak chronić zasoby firmy zarówno w sieci, jak i poza nią.
- **AUTHENTICATOR** zapewnia usługi, które są kluczowe w tworzeniu skutecznej polityki bezpieczeństwa, wzmacniającej ochronę poprzez zapewnienie, że tylko właściwa osoba we właściwym czasie może uzyskać dostęp do wrażliwych sieci i danych.

ENDPOINT SECURITY

EPP (ENDPOINT PROTECTION PLATFORM)

EDR (ENDPOINT DETECTION AND RESPONSE)

XDR (EXTENDED DETECTION AND RESPONSE)

W kontekście zaleceń wynikających z koncepcji Zero Trust Access czy modelu Adaptive Security Architecture Gartnera, prewencja to zdecydowanie za mało. Odpowiedni poziom bezpieczeństwa oferują dopiero rozwiązania klasy EDR (Edpoint Detection and Response), które dzięki mechanizmom analizy zachowań zapewniają funkcjonalność w zakresie:

- WYKRYWANIA URZĄDZEŃ KOŃCOWYCH
- PREDYKCJI ZAGROŻEŃ
- PREWENCJI
- WYKRYWANIA ZAGROŻEŃ W CZASIE RZECZYWISTYM
- USUWANIA ZAGROŻEŃ
- REAKCJI NA ATAKI I DOCHODZENIA
- NAPRAWY SZKÓD I WYCOFYWANIA NIEPOŻĄDANYCH ZMIAN

XDR jest rozszerzeniem EDR o dodatkowe źródła informacji o zagrożeniach. Jest ono rozwiązaniem, które oferuje znacznie więcej niż klasyczna ochrona typu Endpoint Security, mocno zbliżając się do możliwości oferowanych przez rozwiązania klasy Security Operations.

SECURITY OPERATIONS / SOC

Systemy klasy Security Operations, automatyzujące procesy zarządzania bezpieczeństwem, decydują o jakości i skuteczności całego systemu zabezpieczeń. Ich zadaniem jest odciążenie specjalistów w analizach stanu bezpieczeństwa systemu poprzez automatyzację analizy danych zebranych z różnych podsystemów bezpieczeństwa.

SIEM/UEBA

To zaawansowane systemy zarządzania bezpieczeństwem, które automatyzują analizę danych zebranych z podsystemów bezpieczeństwa między innymi poprzez:

- MECHANIZMY LOGUJĄCE
- KORELACJĘ
- ANALIZY BEHAWIORALNE
- UCZENIE MASZYNOWE
- KORZYSTANIE Z WIEDZY DOSTĘPNEJ W CHMURZE

SOAR

Systemy klasy SOAR (Security Orchestration, Automation And Response) stanowią uzupełnienie dla SIEM, zapewniając automatyzację procesów wynikających z analiz dokonanych przez SIEM. Implementacja obu tych rozwiązań jest kluczowa w organizacji SOC (Security Operations Center).

SECURITY AUDIT AND TESTING

Dopełnieniem systemów zabezpieczeń cyfrowych jest wykonywany okresowo i kompleksowo audyt. W jego wyniku identyfikowane są luki bezpieczeństwa, niewykrytych jeszcze przez producentów oprogramowania czy sprzętu. Profesjonalnie przeprowadzone testy bezpieczeństwa zapewniają wczesne wykrycie zagrożeń, w konsekwencji minimalizowanie strat związanych z wystąpieniem cyberataku.

TESTY INFRASTRUKTURY

- TESTY ZEWNĘTRZNE – czyli takie, w których próbujemy uzyskać nieautoryzowany dostęp do danych Twojej firmy, korzystając z sieci zewnętrznej. Takie testy bezpieczeństwa pozwalają wykryć luki w zabezpieczeniach i wdrożyć odpowiednie środki.
- TESTY WEWNĘTRZNE – czyli takie, w których podłączeni do sieci wewnętrznej zbieramy informacje dotyczące działających w niej urządzeń.

TESTY APLIKACJI WEBOWYCH

testy penetracyjne w celu praktycznej oceny bieżącego stanu bezpieczeństwa aplikacji webowej, w szczególności wykrycie wszystkich podatności i odporności na próby przełamania zabezpieczeń, z wykorzystaniem najnowszych technologii.

SOCIAL ENGINEERING

szczególny rodzaj testowania, który opiera się na testach miękkich, związanych ze słabością zasobów ludzkich.

0-DAY

dedykowana usługa, polegająca na wykryciu podatności przed publikacją aktualizacji przez producenta. To nie tylko audyt bezpieczeństwa – to przede wszystkim wysiłek włożony w analizę kodu aplikacji webowych, stron internetowych czy sposobów działania urządzeń sieciowych, w celu znalezienia luki w bezpieczeństwie.

AUDYTY BEZPIECZEŃSTWA - KSC, KRI, SZBI

OCHRONA DANYCH
ZAWSZE I WSZĘDZIE

Sprint
Łączymy Technologie

ZAUFAJ NAM,

PODNIEŚ POZIOM BEZPIECZEŃSTWA TWOJEJ ORGANIZACJI

NASZE MOCNE STRONY

CHCESZ WIEDZIEĆ WIĘCEJ?

Chętnie odpowiemy na wszystkie pytania.

cybersecurity@sprint.pl

OLSZTYN
ul. Jagiellończyka 26
10-062 Olsztyn

+48 89 522 11 00
+48 89 522 11 25
olsztyn@sprint.pl

GDAŃSK
ul. Budowlanych 64E
80-298 Gdańsk

+48 58 340 77 00
+48 58 340 77 01
gdansk@sprint.pl

WARSZAWA
ul. Inflancka 4
00-189 Warszawa

+48 22 826 62 77
+48 22 827 61 21
warszawa@sprint.pl

BYDGOSZCZ
ul. Przemysłowa 15
85-758 Bydgoszcz

+48 52 365 01 01
+48 52 365 01 11
bydgoszcz@sprint.pl