FIREWALL

STRAŻNIK BRZEGU TWOJEJ SIECI

NET COMPLEX

Bezpieczeństwo IT

NET COMPLEX

BEZPIECZEŃSTWO IT

NET COMPLEX
Bezpieczeństwo IT

WEBINARIA

500+ ZREALIZOWANYCH WEBINARIÓW
WARSZTATY ONLINE/ONSITE

NET COMPLEX
Bezpieczeństwo IT

WEBINARIA

AUDYTY

ANALIZA SIECI
AUDYTY BEZPIECZEŃSTWA

NET COMPLEX
Bezpieczeństwo IT

WEBINARIA
AUDYTY
TESTY
PEŁNE WSPARCIE INŻYNIERA
WYSKALOWANE URZĄDZENIE TESTOWE

NET COMPLEX
Bezpieczeństwo IT

WEBINARIA
AUDYTY
TESTY
WDROŻENIA

KOMPLEKSOWE WDROŻENIE W CENIE URZĄDZENIA

NET COMPLEX

Bezpieczeństwo IT

WEBINARIA

AUDYTY

TESTY

WDROŻENIA

SZKOLENIA

CERTYFIKOWANY OŚRODEK SZKOLENIOWY

NET COMPLEX

Bezpieczeństwo IT

WEBINARIA

AUDYTY

TESTY

WDROŻENIA

SZKOLENIA

WSPARCIE

4x CERTYFIKOWANYCH INŻYNIERÓW

NASZE
PORTFOLIO

WatchGuard
TREND MICRO
FUDO SECURITY
XOPERO WORKS, SO YOU CAN TOO!
FORTINET
eset
Forcepoint
VEEAM
STORMSHIELD
panda a WatchGuard brand
safetica
UNITRENDS
Flowmon Driving Network Visibility
Bitdefender
DELL EMC
QNAP
Gigamon®
PROGET
senhasegura
EATON
NACVIEW
ITMANAGER
CYPHER.DOG®
APC

www.netcomplex.pl

FIREWALL

STRAŻNIK BRZEGU TWOJEJ SIECI

FIREWALL

STRAŻNIK BRZEGU TWOJEJ SIECI

BRZEG SIECI

DLACZEGO OCHRONA BRZEGU SIECI JEST WAŻNA?

FIREWALL

STRAŻNIK BRZEGU TWOJEJ SIECI

BRZEG SIECI

ROLA BRZEGU

PIERWSZA LINIA OBRONY
BRAMA DO TWOJEJ ORGANIZACJI
KANAŁ DOSTARCZAJĄCY USŁUGI
PUNKT PRZEPŁYWU DANYCH

FIREWALL

STRAŻNIK BRZEGU TWOJEJ SIECI

BRZEG SIECI

ROLA BRZEGU

MONITORING

MONITORING I ANALIZA ZDARZEŃ

FIREWALL

STRAŻNIK BRZEGU
TWOJEJ SIECI

BRZEG SIECI
FUNKCJONALNOŚĆ
MONITORING

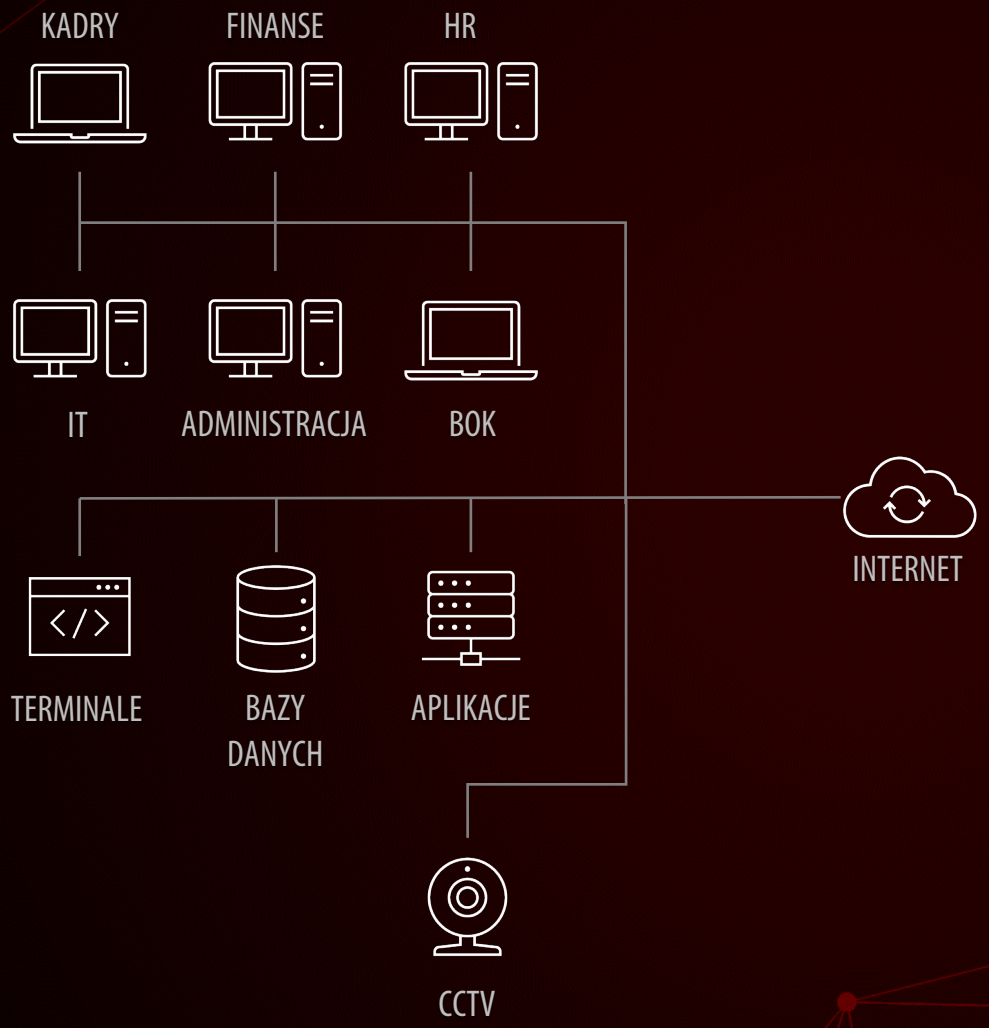
Q&A

BRZEG SIECI

DLACZEGO OCHRONA BRZEGU SIECI JEST WAŻNA?

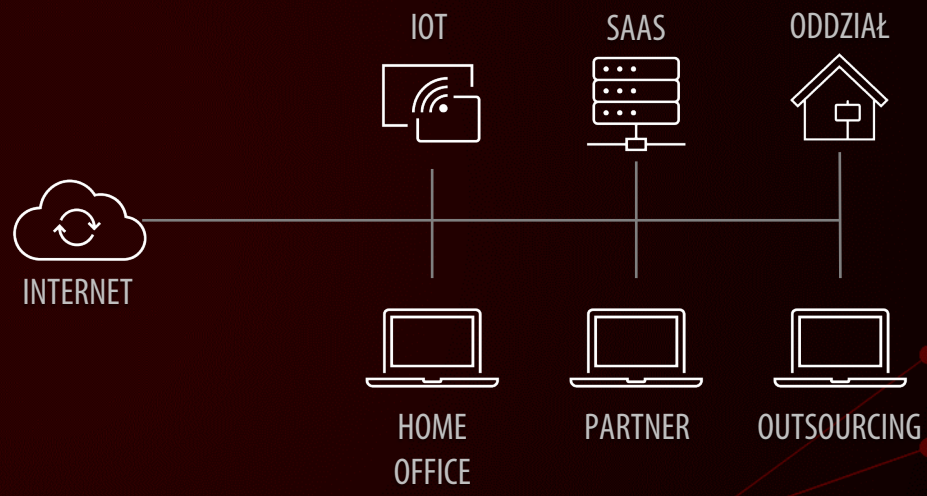
BRZEG SIECI

DLACZEGO OCHRONA BRZEGU SIECI JEST WAŻNA?



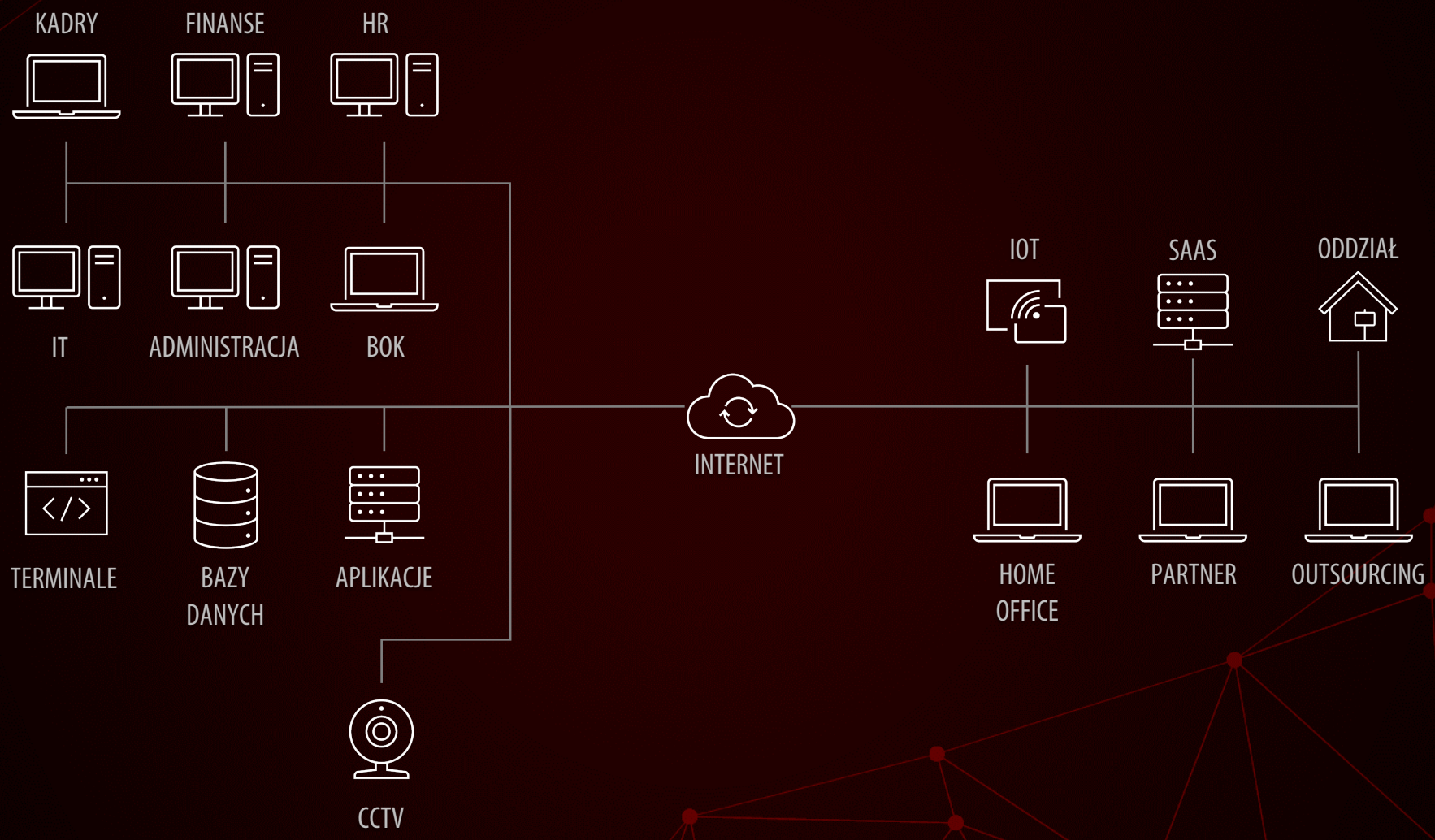
BRZEG SIECI

DLACZEGO OCHRONA BRZEGU SIECI JEST WAŻNA?



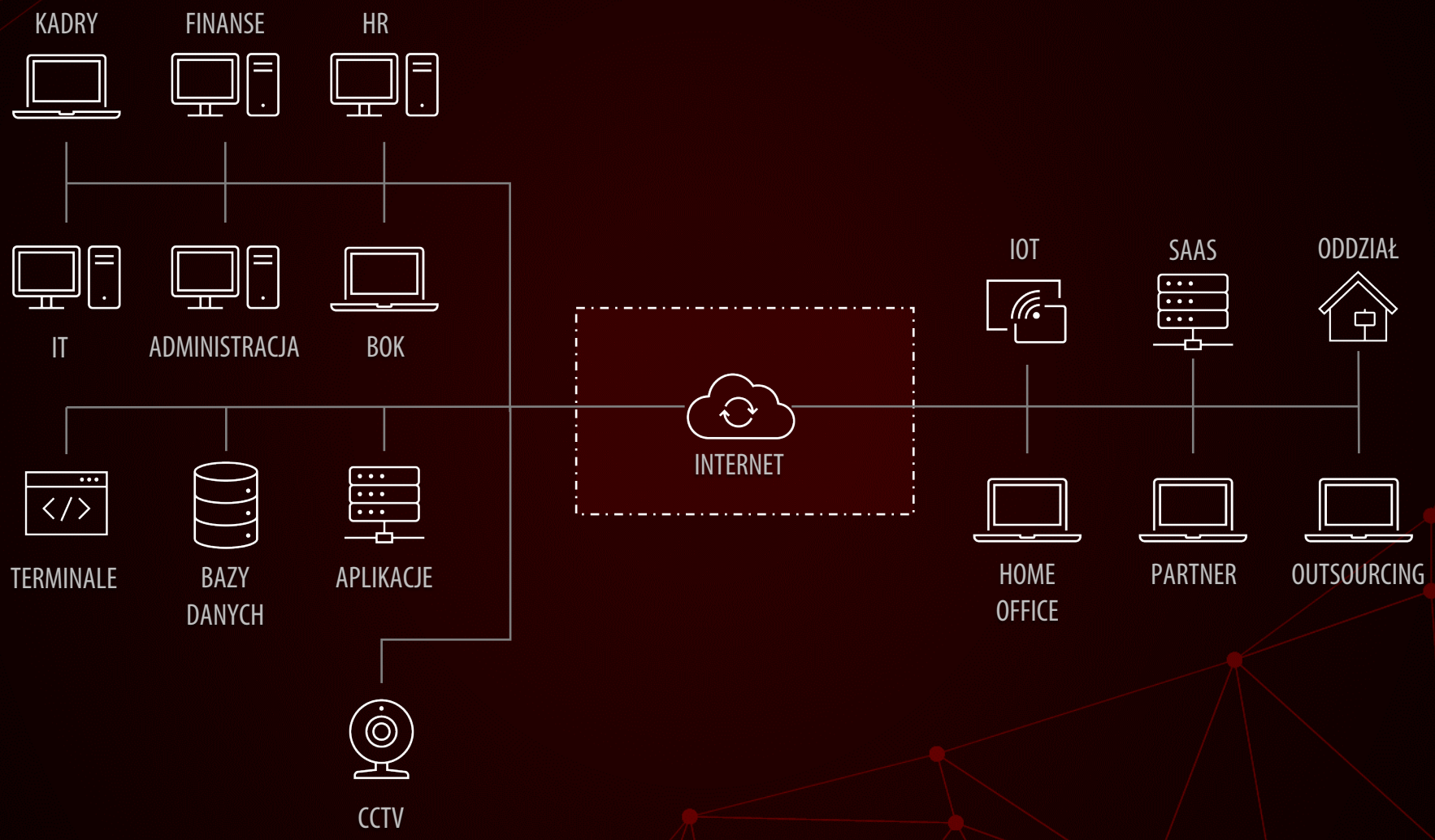
BRZEG SIECI

DLACZEGO OCHRONA BRZEGU SIECI JEST WAŻNA?



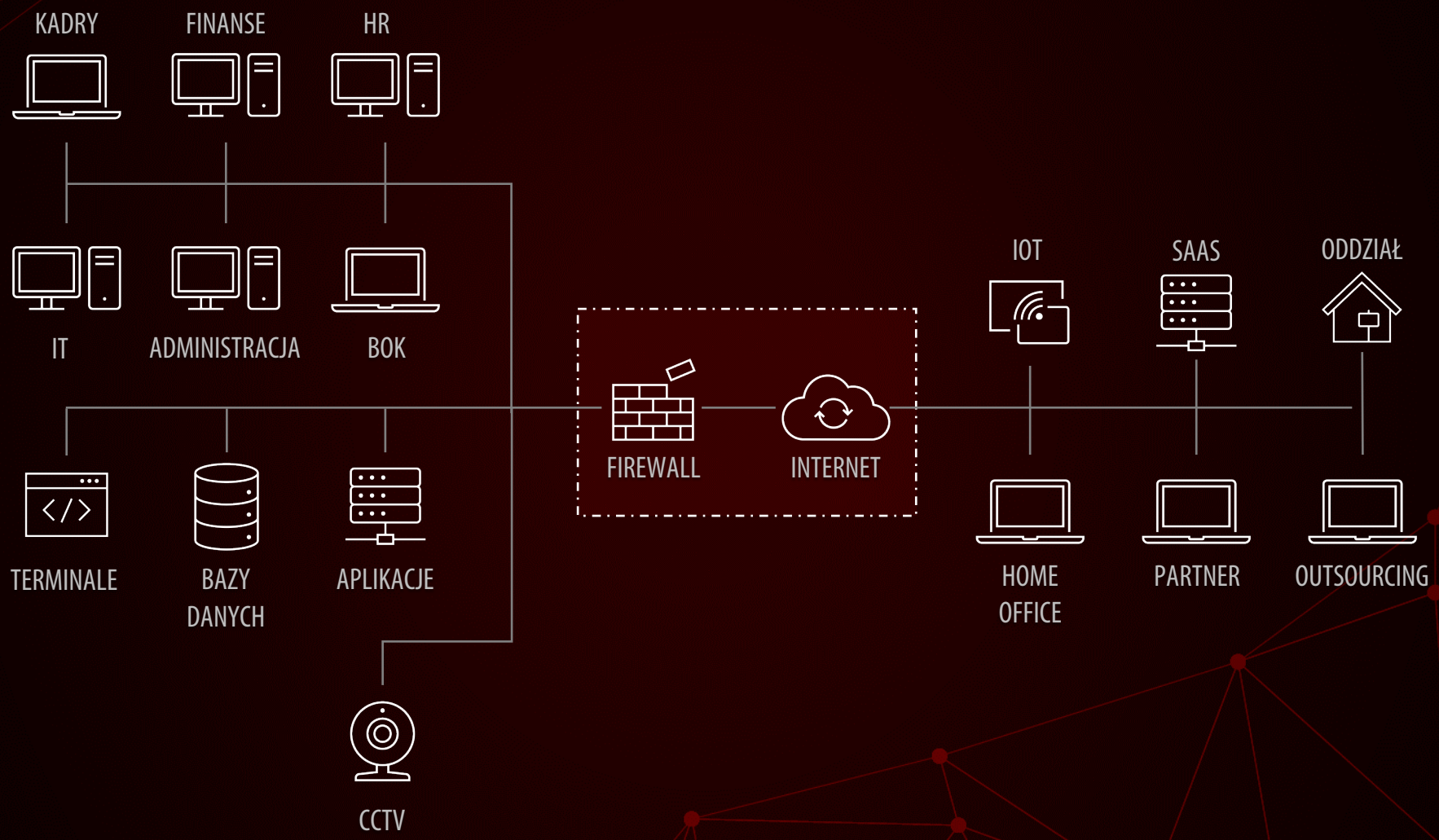
BRZEG SIECI

DLACZEGO OCHRONA BRZEGU SIECI JEST WAŻNA?



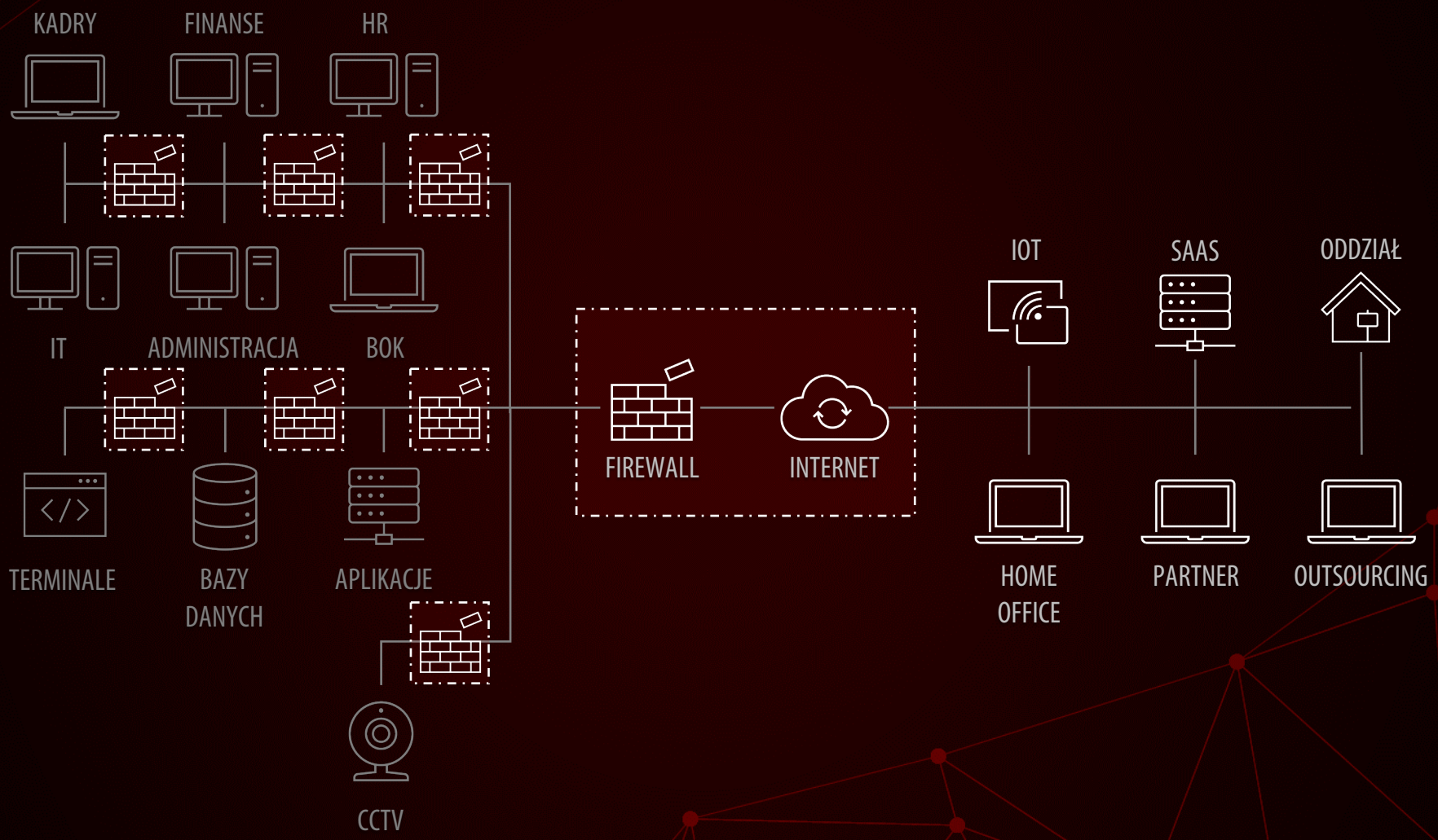
BRZEG SIECI

DLACZEGO OCHRONA BRZEGU SIECI JEST WAŻNA?



BRZEG SIECI

DLACZEGO OCHRONA BRZEGU SIECI JEST WAŻNA?



ROLA BRZEGU

FIREWALL I JEGO ROLE

PIERWSZA LINIA OBRONY

FIREWALL JEST NARZĘDZIEM POZWALAJĄCYM EGZEKWOWAĆ ZASADY BEZPIECZEŃSTWA JEDNOCZEŚNIE PEŁNIĄC ROLĘ SONDY W NASZEJ ORGANIZACJI WYKRYWAJĄC DZIAŁANIA WYKRACZAJĄCE POZA PRZYJĘTY PRZEZ ADMINISTRACJĘ ZAKRES DZIAŁAŃ W SIECI

ZA EGZEKWOWANIE ZASAD BEZPIECZEŃSTWA I WYKRYWANIE INCYDENTÓW ODPOWIADAJĄ MODUŁY PRACUJĄCE W RAMACH ROZWIĄZANIA, KTÓRE PROAKTYWNIE ANALIZUJĄ RUCH SIECIOWY

"GŁÓWNE" FUNKCJONALNOŚCI BEZPIECZEŃSTWA:

- GEOLOKALIZACJA
- BOTNET
- IPS
- KONTROLA APLIKACJI
- FILTROWANIE URL
- ANTYSPAM
- ANTYWIRUS
- INSPEKCJA RUCHU SZYFROWANEGO
- PIASKOWNICA
- KORELACJA ZDARZEŃ

PIERWSZA LINIA OBRONY

- **GEOLOKALIZACJA**
  - BLOKOWANIE KOMUNIKACJI ZE WSKZANYMI KRAJAMI
- **BOTNET**
  - BLOKOWANIE SIECI BOTNET, CZYLI GRUP ZAINFEKOWANYCH KOMPUTERÓW WYKORZYSTYWANYCH DO ATAKÓW
- **IPS**
  - CROSS SITE SCRIPTING NP. ZMODYFIKOWANE LINKI
  - PODATNOŚCI APLIKACJI NP. LOG4SHELL (APACHE), PROXY LOGON (MS EXCHANGE)
  - BRUTE FORCE (RDP)
  - SPYWARE NP. KEYLOGGER
  - SQL INCJECTION NP. UZYSKANIE DOSTĘPU, USUNIĘCIE DANYCH (DROP TABLES)
- **KONTROLA APLIKACJI**
  - WYKRYWANIE NIEPOŻĄDANYCH APLIKACJI BEZ WZGLĘDU TYP RUCHU SIECIOWEGO
    NP. APLIKACJE P2P (TORRENT)
  - KONTROLA WYKORZYSTANIA PASMA NP. OGRANICZENIE YOUTUBE BEZ WZGLĘDU NA SPOSÓB DOSTĘPU (APLIKACJA DEDYKOWANA, WWW)
- **FILTROWANIE URL**
  - ZABLOKOWANIE NIEBEZPIECZNYCH/NIEPOŻADANYCH WITRYN
- **ANTYSPAM**
  - WERYFIKACJA POCZTY W CELU WYELIMINOWANIA NIEPOŻĄDANEJ KORESPONDECJI NP. PHISHING, CEO FRAUD
- **ANTYWIRUS**
  - SKANOWANIE WITRYN, PLIKÓW, ZAŁĄCZNIKÓW NP. WIRUSY, TROJANY, ROBAKI
  - WYKRYWANIE NOWYCH OBIEKTÓW (BEZ SYGNATUR) *TYLKO AI
- **INSPEKCJA RUCHU SZYFROWANEGO**
  - DESZYFRACJA RUCHU DLA UZYSKANIA PEŁNEJ WIDOCZNOŚCI REALIZOWANEGO POŁĄCZENIA
  - PODSTAWA DO SKUTECZNEGO DZIAŁANIA*
- **PIASKOWNICA**
  - PEŁNA EMULACJA SYSTEMU I ANALIZA BEHAWIORALNA W CELU WYKRYCIA ZAGROŻEŃ TYPU 0-DAY, MALWARE, RANSOMWARE
- **KORELACJA ZDARZEŃ**
  - MONITORWANIE Z POZIOMU HOSTÓW W CELU WYKRYCIA ATAKÓW REALIZOWANYCH OD WEWNĄTRZ NP. SABOTAŻ, ZAINFEKOWANY PENDRIVE

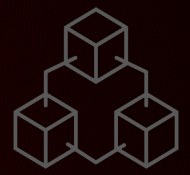
BRAMA DO TWOJEJ ORGANIZACJI

FIREWALL TO BRAMA POZWALAJĄCA ŁĄCZYĆ ROZPROSZONE ORGANIZACJE. ZAPEWNIENIAJĄC ŁATWY I BEZPIECZNY DOSTĘP DLA PRACOWNIKÓW, PARTNERÓW I KLIENTÓW, GDZIEKOLWIEK SIĘ ZNAJDUJĄ.

ZAAWANSOWANE ZAPORY W RAMACH SWOJEJ FUNKCJONALNOŚCI POZWOLĄ GRANULARNIE ZARZĄDZAĆ DOSTĘPEM DO ZASOBÓW W OPARCIU O TOŻSAMOŚĆ UŻYTKOWNIKÓW JEDNOCZEŚNIE IDENTYFIKUJĄĆ CZY SPRZĘT UŻYTY DO KOMUNIKACJI JEST ZAUFANY I ZAAKCEPTOWANY PRZEZ ZESPÓŁ IT. POZWALAJĄC ZABEZPIECZYĆ SIĘ PRZED KONSEKWENCJAMI WYCIEKU DANYCH LOGOWANIA.

KANAŁ DOSTARCZAJĄCY USŁUGI

ZAAWANSOWANY FIREWALL AUTOMATYCZNIE WYŚLE RUCH WRAŻLIWY NA OPÓŹNIENIA O WYSOKIM PRIORYTECIE, TAKI JAK VOIP I WIDEOKONFERENCJE, PRZEZ ŁĄCZE INTERNETOWE O WYŻSZEJ JAKOŚCI. JEDNOCZEŚNIE REALIZUJĄC POŁĄCZENIA O NIŻSZYM PRIORYTECIE PRZEZ MNIEJ WYDAJNE ŁĄCZE W OPARCIU O PROGI WYDAJNOŚCI TAKIE JAK OPÓŹNIENIE, ZMIENNOŚĆ OPÓŹNIENIA CZY UTRATĘ PAKIETÓW



ZAPEWNIENIE BEZPROBLEMOWEGO, NIEPRZERWANEGO DOSTĘPU DO USŁUG DLA PRACOWNIKÓW, PARTNERÓW, KLIENTÓW CZY URZĄDZEŃ IOT GDZIEKOLWIEK SIĘ ZNAJDUJĄ, JEST JEDNĄ Z KLUCZOWYCH KWESTI.

SIEĆ GORSZEJ JAKOŚCI BĘDZIE POWODOWAĆ OBNIŻENIE POZIOMU USŁUG ŚWIADCZONYCH ODBIORCOM.

PUNKT PRZEPŁYWU DANYCH

BRZEG SIECI TO OPTYMALNE MIEJSCE DO MONITORINGU SIECI POZWALAJĄCE ZROZUMIEĆ, CO DZIEJE SIĘ W NASZEJ SIECI. W SIECIACH ROZPROSZONYCH TYLKO FIREWALL MA WGLĄD W CAŁOŚC RUCHU DZIĘKI CZEMU ANALIZA ZDARZEŃ PRZEDSTAWI SZERSZĄ PERSPEKTYWĘ

NA PODSTAWIE DANYCH O UŻYTKOWNIKACH, APLIKACJACH, URZĄDZENIACH I ZAGROŻENIACH PRZEDSIĘBIORSTWA MOGĄ UZYSKIWAĆ INFORMACJE POMOCNE PRZY PODEJMOWANIU LEPSZYCH DECYZJI DOTYCZĄCYCH MIN. WSPARCIA PRACOWNIKÓW, OGRANICZANIA RYZYKA I KOSZTÓW.

BEZ ODPOWIEDNIEGO POZIOMU SZCZEGÓŁOWOŚCI DANE STAJĄ SIĘ WYPACZONE I NIEMIARODAJNE.

MONITORING

DLACZEGO DANE SAME W SOBIE NIE MAJĄ WARTOŚCI

DANE SAME W SOBIE NIE SĄ WARTOŚCIOWE.
WARTOŚĆ TKWI W ANALIZIE
PRZEPROWADZONEJ NA DANYCH
ORAZ W PRZEKSZTAŁCENIU ICH W
INFORMACJĘ.

KOSZT BRAKU WIDOCZNOŚCI

SIEĆ BRZEGOWA ZAWIERA WIELE INFORMACJI DOTYCZĄCYCH UŻYTKOWNIKÓW, ICH URZĄDZEŃ, APLIKACJI, Z KTÓRYCH KORZYSTAJĄ, MIEJSC, KTÓRE ODWIEDZAJĄ, A NAWET INFORMACJI O OBSZARACH, W KTÓRYCH WYSTĘPUJĄ POTENCJALNE ZAGROŻENIA.

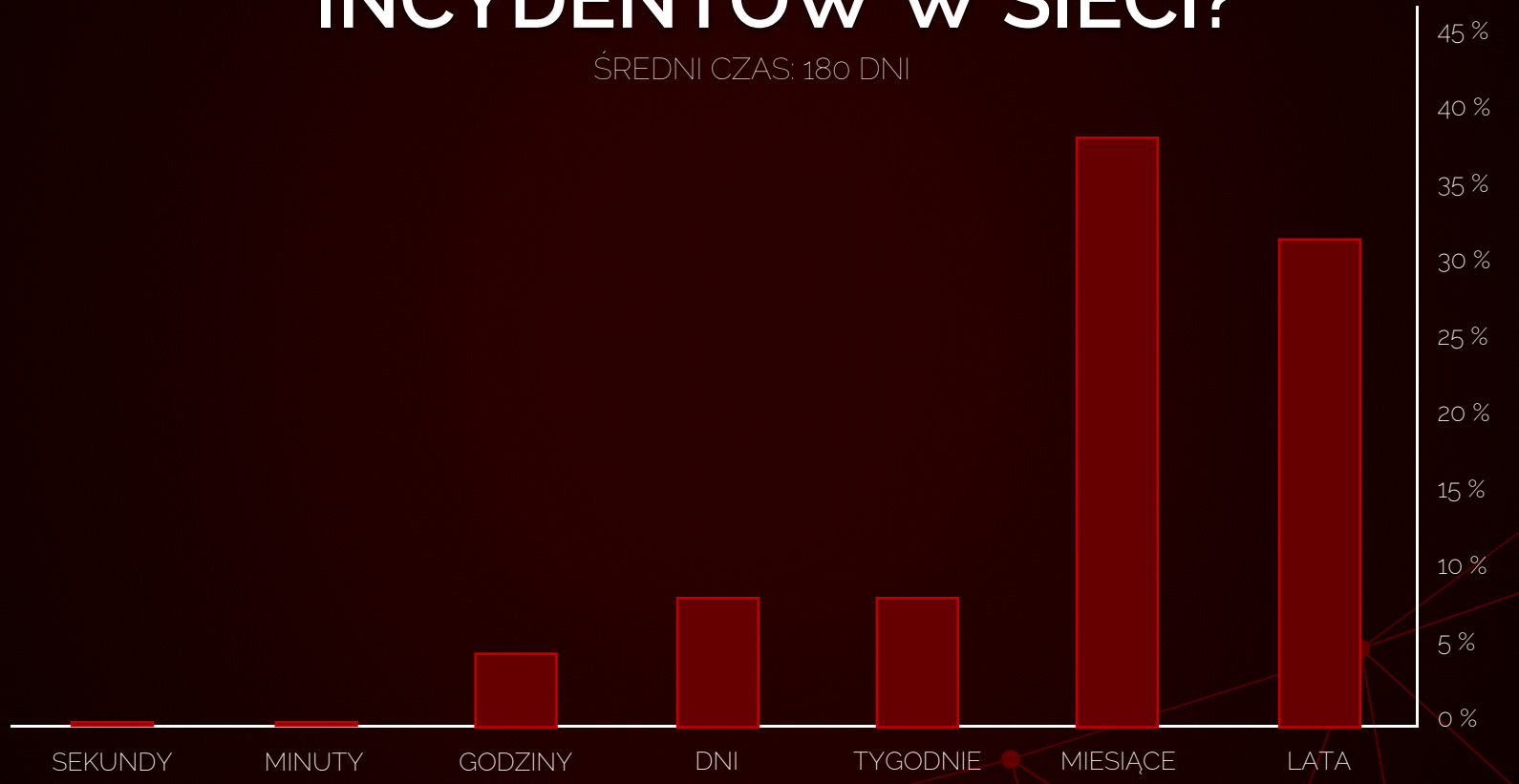
BEZ TEJ WIDOCZNOŚCI ORGANIZACJA MOŻE SPĘDZIĆ NIEZLICZONE GODZINY, PRÓBUJĄC ZROZUMIEĆ, W JAKI SPOSÓB UŻYTKOWNICY WCHODZĄ W INTERAKCJE ZE SWOIM OTOCZENIEM, JAK UZYSKUJĄ DOSTĘP DO INFORMACJI I JAK JE KONSUMUJĄ, A NAWET PRZEOCZYĆ POTENCJALNE ZAGROŻENIE, KTÓRE MOŻNA BYŁO ZMINIMALIZOWAĆ ODPOWIEDNIO WCZEŚNIE.

KOSZT APLIKACJI ISTOTNYCH DLA DZIAŁALNOŚCI FIRMY, KTÓRE NIE ZAADAPTOWAŁY SIĘ WŚRÓD PRACOWNIKÓW. WIELE ORGANIZACJI INWESTUJE POWAŻNY ODSETEK SWOJEGO BUDŻETU W NOWE APLIKACJE I SYSTEMY MAJĄCE ZA ZADANIE ZWIĘKSZENIE WYDAJNOŚCI. JEŻELI PRACOWNICY MAJĄ NIEDOBRE DOŚWIADCZENIA Z TAKIMI APLIKACJAMI LUB USŁUGAMI, NIE BĘDĄ CHCIELI Z NICH KORZYSTAĆ, A WTEDY ZWROT Z INWESTYCJI GWAŁTOWNIE SPADNIE.

KOSZT NARUSZENIA BEZPIECZEŃSTWA. W PRZYPADKU WIELU ORGANIZACJI WŁASNOŚĆ INTELEKTUALNA I ZASOBY SĄ PODSTAWĄ ICH FUNKCJONOWANIA. JAKIE MOGĄ BYĆ NASTĘPSTWA, JEŻELI WPADNĄ W NIEPOWOŁANE RĘCE? ORGANIZACJE PRZESTĘPCZE ODZNACZAJĄ SIĘ BIEGŁOŚCIĄ W CZERPANIU ZYSKÓW Z CUDZEJ WŁASNOŚCI INTELEKTUALNEJ I DANYCH POPRZEZ ŻĄDANIE OKUPU, WYMUSZENIA LUB ODSPRZEDAŻ OFERUJĄCEMU NAJWYŻSZĄ CENĘ.

JAK DŁUGO ZAJMUJE ODKRYCIE INCYDENTÓW W SIECI?

ŚREDNI CZAS: 180 DNI



NET COMPLEX
Bezpieczeństwo IT

DZIĘKUJE ZA UWAGĘ

PIOTR MROWIEC
INŻYNIER WSPARCIA TECHNICZNEGO

p.mrowiec@netcomplex.pl