CYBERCLUE

CYBERBEZPIECZEŃSTWO DLA KAŻDEJ FIRMY

www.cyberclue.tech | +48 882 764 675 | info@cyberclue.tech

ZESPÓŁ EKSPERTÓW

W **Cyber**Clue mamy silny zespół IT z certyfikatami CompTIA Sec+, ale również osoby z doświadczeniem w komunikacji i szkoleniach.

Zespół IT posiada kompetencje developerskie (Fullstack), Reverse Engineering (firmware, software, malware), Exploit Development, Threat Intelligence, Pentesting oraz Digital Forensic.

KORZYŚCI ZE WSPÓŁPRACY Z CYBERCLUE

1. Doświadczeni eksperci z obszaru cyberbezpieczeństwa
2. Monitorowanie zarówno automatyczne przy użyciu systemów, jak też manualne, wykonywane przez ekspertów CyberClue
3. Minimalizacja ryzyka udanego ataku
4. Alerty odnośnie nowych i wschodzących zagrożeń
5. Jasne i czytelne raporty stanu bezpieczeństwa oraz wsparcie we wdrożeniu rekomendacji
6. Stałe szkolenia i podnoszenie świadomości pracowników

CYBERCLUE

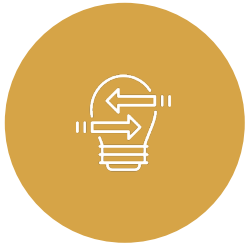
NAJWAŻNIEJSZE WYZWANIA DLA FIRM

ZAPEWNIENIE CIĄGŁOŚCI DZIAŁANIA

Codziennie ataki hackerskie powodują zatrzymanie działalności firm – produkcji, sklepów internetowych, systemów obsługujących klientów, nawet ratujących życie.

UTRZYMANIE STAŁEGO DOSTĘPU DO SYSTEMÓW INFORMATYCZNYCH

Systemy IT to podstawa działania większości firm. Zablokowanie ich działania to problemy lub uniemożliwienie obsługi klientów lub nawet zablokowanie działania całej firmy.



GWARANCJA AUTOMATYZACJI DZIAŁAŃ

Wiele firm ma zautomatyzowane w całości lub części procesy produkcyjne i biznesowe. W przypadku ataku prace, które wcześniej były zautomatyzowane, muszą być wykonywanie manualnie. Może to spowodować tylko opóźnienia, ale również spadek jakości, niedotrzymanie standardów lub nawet zagrożenie życia klientów.

WIZERUNEK FIRMY GODNEJ ZAUFANIA

Przez lata budujemy pozycję firmy na rynku. Wyciek wrażliwych danych, zablokowanie dostępu do usług, opóźnienia czy obniżenie jakości z powodu ataku może na zawsze zniweczyć nasze wieloletnie działania w tym zakresie.

CYBERCLUE

WSPARCIE BEZPIECZEŃSTWA

AUDYT BEZPIECZEŃSTWA

1. Weryfikacja bezpieczeństwa istniejących systemów i oprogramowania
2. Zgłoszenie ewentualnych poprawek w ramach obowiązujących gwarancji

SKANY I TESTY PENETRACYJNE

1. Sprawdzenie bezpieczeństwa technologicznego
2. Sprawdzenie świadomości pracowników
3. Jasne i czytelne raporty stanu bezpieczeństwa

STAŁA OBSŁUGA

1. Monitorowanie potencjalnie niebezpiecznych zdarzeń w celu zapobieżenia atakom
2. Regularne testy penetracyjne
3. Testy penetracyjne przy zmianach w infrastrukturze
4. Szybka reakcja na incydenty

CYBERCLUE

ZWIĘKSZANIE ŚWIADOMOŚCI PRACOWNIKÓW

TESTY SOCJOTECHNICZNE

1. Sprawdzenie, w jakich obszarach pracownicy są świadomi niebezpieczeństw IT
2. Określenie luk
3. Sprawdzenie reakcji na podejrzane zachowania
4. Uświadomienie niebezpieczeństw

SZKOLENIA

1. Obrazowe pokazanie pracownikom: niebezpieczeństw, metod zwiększania bezpieczeństwa oraz możliwych konsekwencji ataków
2. E-Learing - cyberbezpieczeństwo i bezpieczeństwo informacji
3. Cybersecurity College – prowadzony przez ekspertów z Izraela
4. Rozwój pracowników: mentoring technologiczny

KAMPANIE PODNOSZĄCE ŚWIADOMOŚĆ

1. Stałe edukowanie pracowników
2. Utrzymywanie czujności
3. Zwiększanie świadomości
4. Angażowanie pracowników w bezpieczeństwo

CYBERCLUE

AUDYTY I ZARZĄDZANIE RYZYKIEM

AUDYT PROCESÓW

1. Zarządzenie bezpieczeństwem informacji
2. Zarządzanie ciągłością działania
3. Ochrona Danych osobowych
4. Bezpieczeństwo fizyczne

AUDYTY ZGODNOŚCI

1. ISMS/SZBI wg. ISO 27001
2. BCMS/SZCD wg. ISO 22301
3. Zgodność z Ustawą o Krajowym Systemie Cyberbezpieczeństwa
4. Zgodność z GDPR/RODO

ZARZĄDZANIE RYZYKIEM

1. Szkolenia i warsztaty analizy ryzyka (wg. ISO27005 / ISO31000)
2. Szkolenia i warsztaty BIA (wg. ISO 22301)

CYBERCLUE

SZEROKIE WSPRACIE DLA FIRM

WDROŻENIA SYSTEMÓW ZARZĄDZANIA

1. ISMS/SZBI wg. ISO 27001
2. Opracowanie / aktualizacja dokumentacji ISMS/SZBI
3. Opracowanie Strategii Bezpieczeństwa
4. BCMS/SZCD wg. ISO 22301
5. Opracowanie planów ciągłości, odtworzeniowych oraz planów testów
6. Zgodność z Ustawą o Krajowym Systemie Cyber Bezpieczeństwa
7. Zgodność z GDPR/RODO

LICENCJONOWANE NARZĘDZIA

Oprogramowanie do monitoringu darkwebu. Automatycznie zbiera, analizuje, monitoruje i ostrzega o pojawiających się zagrożeniach.

1. Alerty o zagrożeniach w czasie rzeczywistym
2. Zalecenia dot. łagodzenia skutków
3. Monitoring potencjalnych wycieków danych firmowych w różnych źródłach

USŁUGI DODATKOWE

1. Monitoring darkwebu – sprawdzanie wycieków danych i identyfikacja potencjalnych ataków
2. Mentoring technologiczny
3. Obsługa incydentów naruszenia bezpieczeństwa – Incident response
4. Informatyka śledcza - Digital Forensic
5. Ubezpieczenia cybersecurity

CYBERCLUE

TESTY PENETRACYJNE

Testy penetracyjne to symulowane ataki na środowisko IT.
Podczas testów wykorzystujemy narzędzia oraz metody, z których korzystają cyberprzestępcy.

Zakres testów:

- Endpointy
- Infrastruktura IT
- Urządzenia IoT
- Aplikacje i systemy
- Systemy przemysłowe SCADA

Wynikiem testów jest czytelny raport ze zidentyfikowanymi obszarami do poprawy bezpieczeństwa, ze wskazaniem poziomów ryzyka.
CyberClue może również pomóc w zaimplementowaniu rekomendowanych zmian.

CYBERCLUE

STAŁE WSPARCIE W ZAPEWNIENIU BEZPIECZEŃSTWA IT (SOC)

Raz sprawdzona infrastruktura nie pozostaje bezpieczna.

Kluczem do podwyższenia bezpieczeństwa jest stałe jej monitorowanie.
Powodem są ciągłe zmiany i nowe rodzaje ataków przeprowadzanych przez cyberprzestępców.

Zakres działań:

- Monitoring endpointów
- Proaktywna identyfikacja pojawiających się podatności
- Monitoring infrastruktury IT
- Okresowo przeprowadzane wewnętrzne audyty bezpieczeństwa w celu zapewnienia ciągłości działania i integralności danych
- Aktywne wykrywanie incydentów
- Szybka reakcja specjalistów w przypadku ataku
- Szkolenia i kampanie zwiększające świadomość pracowników

CYBERCLUE | **SZKOLENIA**

- Szkolenia ogólne oraz specjalistyczne dla określonych stanowisk
- Kompleksowe ujęcie pojęcia cyberbezpieczeństwa w firmie
- Przeprowadzane na platformie e-learningowej
- Teoria + praktyka - przykłady - na koniec test i certyfikat

Sprawdź swoją wiedzę

Przeczytaj uważnie pytania i odpowiedz by zdobyć certyfikat modułu bezpieczeństwo fizyczne!

Ready to Start!

PRZYJAZNA PLATFORMA SZKOLENIOWA

3. Zagubiony zewnętrzny nośnik pamięci - co może być konsekwencją?

- Konsekwencjami takiego zachowania może być utrata danych firmowych lub prywatnych, ale także konsekwencje wynikające z ujawnieniem danych niejawnych lub incydent RODO.

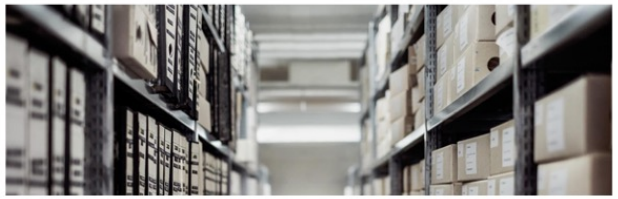
Pamiętaj!

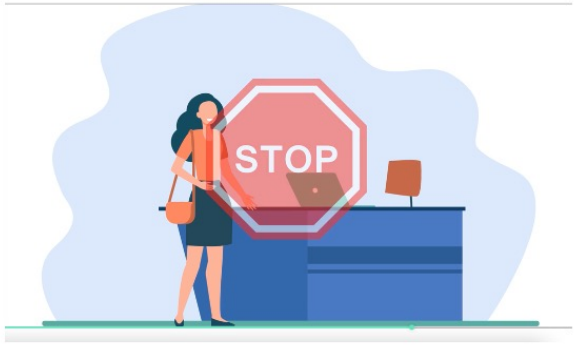
- Nigdy nie używaj pendrive z nieznajomego źródła na swoim lub firmowym komputerze

- Nie używaj tego samego pendrive do celów prywatnych i służbowych

6. W jaki sposób utylizujesz dokumenty?

Gdy dokumenty docierają do końca swojego cyklu użycia - często musimy je zutylizować - ważne jest to by wykonać to w odpowiedni sposób - **dokumenty nie powinny być w całości wyrzucane do śmieci, by nie narazić firmy na wyciek danych - dokumenty powinny być zniszczone przy użyciu niszczarki.**





KAMPANIA PODNOSZĄCA ŚWIADOMOŚĆ

- Czas trwania: 6 m-cy
- Częstotliwość aktywności: 2 serie/m-c
- Koncepcja: gaming

- Zbieranie punktów: indywidualne i zespołowe
- Co miesiąc: TOP 3 osoby i TOP 3 zespoły z małymi nagrodami
- Na koniec duże nagrody i event związany z cyberbezpieczeństwem: spotkanie z testerem, atak na żywo

CEL:

stworzenie ekscytacji tematem cyberbezpieczeństwa poprzez wzbudzenie poczucia rywalizacji pomiędzy zespołami i współpracy w zespołach

Nagrody z dowcipnymi
(dla rozumiejących temat)
napisami kreują poczucie
„JA ROZUMIEM – JESTEM FAJNA/Y"

CyberClue Sp. z o.o.

Agnieszka Grostal

V-ce Prezes ds. Sprzedaży

+48 882 7664 675

agnieszka.grostal@cyberclue.tech