Polityka organizująca Computer Security Incident Response Team SPRINTTECH

Zgodnie z RFC2350

SPIS TREŚCI

1. Wstęp

Z przyjemnością przedstawiamy Sprinttech Sp z o.o., lidera w dziedzinie cyberbezpieczeństwa i ochrony informacji. W czasie trwania działalności, zdobyliśmy zaufanie klientów z różnych sektorów przemysłu oraz instytucji rządowych. Nasza misja to dostarczanie kompleksowych i innowacyjnych rozwiązań w dziedzinie cyberbezpieczeństwa, aby pomóc naszym klientom w ochronie ich aktywów, danych i reputacji przed zagrożeniami związanymi z cyberprzestrzenią.

Nasza oferta usług obejmuje:

1.1. Centrum Operacji Cybernetycznych (CSIRT SOC)

Nasze Centrum Operacji Cybernetycznych (SOC) to serce naszej działalności w dziedzinie cyberbezpieczeństwa. Nasz wysoce wykwalifikowany zespół analityków monitoruje, wykrywa i reaguje na wszelkie zagrożenia związane z cyberprzestrzenią w czasie rzeczywistym. Dzięki zaawansowanym narzędziom i technologiom, oferujemy usługi SOC, które pozwalają naszym klientom na skuteczną ochronę przed atakami, a także na szybką reakcję w przypadku incydentów.

1.2. Testy Penetracyjne

Nasze testy penetracyjne są przeprowadzane przez doświadczonych specjalistów, którzy wykorzystują zaawansowane techniki, aby zidentyfikować słabości i ryzyka w infrastrukturze IT i aplikacjach naszych klientów. Dzięki tym usługom nasi klienci mogą zwiększyć poziom swojego bezpieczeństwa, eliminując potencjalne luki w zabezpieczeniach, zanim zostaną wykorzystane przez potencjalnych atakujących.

1.3. Audyty Bezpieczeństwa

Nasi eksperci w dziedzinie audytu bezpieczeństwa przeprowadzają szczegółowe oceny środowiska IT naszych klientów, identyfikując ryzyka i dostarczając rekomendacji dotyczących zwiększenia poziomu bezpieczeństwa. Nasze audyty obejmują zarówno infrastrukturę sieciową, jak i aplikacje, a ich celem jest dostarczenie pełnej analizy, która pozwala naszym klientom na wdrożenie efektywnych środków ochronnych.

Jesteśmy dumni z naszej zdolności do dostarczania najwyższej jakości usług w dziedzinie cyberbezpieczeństwa i reagowania na incydenty. Nasz zespół skupia się na indywidualnych potrzebach każdego klienta, dostarczając rozwiązania dostosowane do ich specyficznych wyzwań i celów biznesowych.

Zapraszamy do zapoznania się z naszą ofertą i skorzystania z naszych usług, które pomogą Państwa organizacji w osiągnięciu maksymalnego poziomu bezpieczeństwa w zmieniającym się i coraz bardziej wymagającym środowisku cybernetycznym.

Jeśli mają Państwo pytania lub potrzebują dodatkowych informacji, prosimy o kontakt z naszym zespołem. Jesteśmy gotowi, aby wesprzeć Państwa organizację w zapewnieniu skutecznej ochrony przed zagrożeniami związanymi z cyberprzestrzenią.

Serdecznie zapraszamy do współpracy ze Sprinttech!

2. Cele

2.1. Identyfikacja i Wykrywanie Incydentów:

Głównym celem CSIRT Sprinttech jest identyfikacja i wykrywanie wszelkich incydentów związanych z bezpieczeństwem informatycznym, które mogą wystąpić w organizacji. To obejmuje ataki, naruszenia, awarie oraz inne zagrożenia.

2.2. Szybka Reakcja:

CSIRT Sprinttech dąży do zapewnienia szybkiej i skutecznej reakcji na incydenty. Celem jest minimalizacja skutków incydentów poprzez natychmiastowe działania.

2.3. Analiza i Ocena Zagrożeń:

CSIRT Sprinttech przeprowadza analizy incydentów, aby zrozumieć ich źródło, skutki oraz sposób działania. Cel to określenie rodzaju zagrożenia i okoliczności, które pozwolą na lepsze zabezpieczenie się przed podobnymi incydentami w przyszłości.

2.4. Ochrona Aktywów:

CSIRT Sprinttech ma za zadanie ochronę aktywów organizacji, w tym danych, systemów, sieci i innych zasobów przed potencjalnymi zagrożeniami.

2.5. Zapobieganie Powtórnym Incydentom:

W ramach działań CSIRT Sprinttech podejmuje kroki w celu zapobiegania powtórnym incydentom. To może obejmować wprowadzanie środków ochronnych, poprawianie procedur czy edukację pracowników.

2.6. Współpraca i Informowanie:

CSIRT Sprinttech dąży do skutecznej współpracy z innymi zespołami reagowania na incydenty, organizacjami branżowymi oraz organami ścigania. Ponadto, informuje on zarząd, personel oraz zainteresowane strony o incydentach i środkach zaradczych.

2.7. Zwiększenie Świadomości Bezpieczeństwa:

CSIRT Sprinttech promuje świadomość bezpieczeństwa w organizacji poprzez edukację pracowników, dostarczanie informacji o bieżących zagrożeniach oraz zachęcanie do przestrzegania polityk i procedur bezpieczeństwa.

2.8. Nadzór i Monitorowanie:

CSIRT Sprinttech nadzoruje środowisko IT organizacji w celu wczesnego wykrywania i zapobiegania incydentom oraz zagrożeniom.

2.9. Doskonalenie Umiejętności:

CSIRT Sprinttech stara się ciągle podnosić swoje umiejętności i wiedzę, aby skutecznie reagować na coraz bardziej zaawansowane zagrożenia związane z cyberbezpieczeństwem.

2.10. Dokumentacja i Analiza Incydentów:

CSIRT Sprinttech jest odpowiedzialny za dokładną dokumentację incydentów oraz przeprowadzanie analiz powłamaniowej, które pomagają organizacji w unikaniu podobnych sytuacji w przyszłości.

3. Struktura i role

3.1. Dyrektor techniczny CSIRT:

- Zarządza całym zespołem CSIRT.
- Odpowiada za koordynację działań i podejmowanie strategicznych decyzji w zakresie reagowania na incydenty.
- Utrzymuje kontakt z zarządem organizacji.

3.2. Analitycy Incydentów (Incident Analysts):

- Monitorują i wykrywają incydenty związane z cyberbezpieczeństwem w czasie rzeczywistym.
- Przeprowadzają analizy incydentów, identyfikując źródło i charakter ataku.
- Oceniają ryzyko i skutki incydentów.

3.3. Specjaliści ds. Reagowania na Incydenty (Incident Responders):

- Są odpowiedzialni za natychmiastowe reagowanie na incydenty.
- Izolują i likwidują zagrożenie, przywracając normalne funkcjonowanie systemów.
- Przeprowadzają działania mające na celu ograniczenie skutków incydentu.

3.4. Specjaliści ds. Analizy Zagrożeń (Threat Analysts):

- Przeprowadzają analizy zagrożeń i działają na rzecz zrozumienia taktyk, technik i procedur używanych przez potencjalnych atakujących.
- Pomagają w identyfikacji potencjalnych ryzyk i luk w zabezpieczeniach.

3.5. Specjaliści ds. Audytu Bezpieczeństwa (Security Auditors):

- Przeprowadzają audyty bezpieczeństwa w organizacji, identyfikując słabości i ryzyka.
- Rekomendują środki zaradcze i poprawki w celu wzmocnienia ochrony.

3.6. Eksperci ds. Testów Penetracyjnych (Penetration Testers):

- Przeprowadzają testy penetracyjne, aby ocenić odporność infrastruktury na ataki.
- Pomagają w identyfikacji luk w zabezpieczeniach, które mogą być wykorzystane przez potencjalnych atakujących.

3.7. Specjaliści ds. Budowania Świadomości Cyberbezpieczeństwa (Security Trening and Awareness Specialists):

- Odpowiadają za edukację pracowników organizacji w zakresie bezpieczeństwa informatycznego.
- Promują świadomość bezpieczeństwa wśród pracowników.

3.8. Koordynator Komunikacji (Communication Coordinator):

- Zarządza komunikacją wewnętrzną i zewnętrzną w przypadku incydentów.
- Informuje pracowników, interesariuszy oraz media o bieżących incydentach i działaniach CSIRT Sprinttech.

3.9. Specjaliści ds. Dokumentacji (Documentation Specialists):

- Zarządzają dokumentacją związaną z incydentami, analizami zagrożeń i działaniami reakcyjnymi.
- Pomagają w tworzeniu raportów i dokumentacji wewnętrznej oraz zewnętrznej.

3.10. Radcy Prawni (Legal Advisors):

- Zapewniają wsparcie prawnego w przypadku incydentów, w szczególności w kwestiach związanych z przepisami dotyczącymi prywatności i cyberbezpieczeństwa.

3.11. Zarząd i Dyrekcja (Management and Leadership):

- Zarząd odpowiada za kierownictwo organizacji,
- Współpracuje z CSIRT Sprinttech w podejmowaniu strategicznych decyzji dotyczących bezpieczeństwa informatycznego i alokacji zasobów.

4. Proces reagowania na incydenty

4.1. Zgłoszenie Incydentu: Incydent może być zgłaszany na różne sposoby, w tym drogą:

A. mailową,
B. telefoniczną,
C. automatycznie generowany przez systemy monitorujące.
D. Generowane w wyniku pracy Threat Hunterów/ SOC Operatorów
E. Incydenty zgłoszone drogą mailową lub telefoniczną trafiają do SOC Operatorów.

4.2. Priorytetyzacja Zgłoszeń:

A. SOC Operatorzy nadają odpowiedni priorytet zgłoszeniu, uwzględniając jego charakter, skomplikowanie i wpływ na organizację.
B. Priorytetyzacja odbywa się w Systemie Obsługi Incydentów Sprinttech (SOiS).

4.3. Analiza Zgłoszeń:

A. SOC operatorzy wsparci systemami do monitorowania i analizy przeprowadzają wstępną analizę zgłoszeń, identyfikując ich źródło i potencjalne zagrożenia.

4.4. Wykrycie Incydentu:

A. W przypadku wykrycia incydentu noszącego znamiona krytycznego lub zgłoszenia telefonicznego i mailowego odbywa się Spotkanie Zespołu Specjalistów ds. Reagowania na Incydenty (Incident Responders), Specjaliści ds. Analizy Zagrożeń (Threat Analysts) i Koordynator Komunikacji w celu omówienia zgłoszenia.
B. Celem spotkania jest określenie skali i charakteru incydentu oraz opracowanie planu działań (remediacji).
C. W przypadku incydentów wykrytych na poziomie systemów do monitorowania decyzję o priorytecie oraz eskalacji zgłoszenia podejmuje przyjmujący SOC Operator

4.5. Rekomendacje i Plan Remediacji:

A. Podczas spotkania zespołu ds. Reagowania na Incydenty ustalane są rekomendacje i plan remediacji, które pomogą w ograniczeniu zagrożenia.
B. Rekomendacje te mogą obejmować techniczne środki zaradcze, zmiany w politykach bezpieczeństwa lub inne działania.

4.6. Komunikacja ze Zgłaszającym:

A. W przypadku zgłoszeń drogą mailową lub telefoniczną oraz incydentów krytycznych, CSIRT komunikuje się ze zgłaszającym w celu omówienia incydentu i planu remediacji.
B. CSIRT Sprinttech zapewnia bieżące informacje na temat postępów remediacji i aktualizacji dotyczących incydentu.

4.7. Implementacja Planu Remediacji:

A. CSIRT wdraża plan remediacji możliwie najszybciej (stosując również rozwiązania automatyczne), zgodnie z ustalonymi priorytetami i SLA oraz umowami.

4.8. Monitoring i Aktualizacje:

A. CSIRT nadzoruje postępy działań remediacji oraz monitoruje środowisko w celu wykrycia ewentualnych kolejnych zagrożeń.

B. Aktualizuje zgłaszającego w miarę postępów i zmian w incydencie.

4.9. Zakończenie Incydentu:

A. Incydent uznaje się za zakończony, gdy wszystkie działania remediacji są zaimplementowane i/lub ryzyko jest akceptowalne.

B. CSIRT może również przeprowadzić analizę powłamaniową, aby zrozumieć przyczyny incydentu i dostosować strategię bezpieczeństwa.

Proces reagowania na incydenty CSIRT Sprinttech uwzględnia różne źródła zgłoszeń, priorytetyzację, analizę, rekomendacje oraz działania remediacji, a także aktywną komunikację z klientami. To kluczowe elementy zapewniające efektywność działalności CSIRT i ochronę organizacji przed zagrożeniami związanymi z cyberbezpieczeństwem.

5. Raportowanie incydentów

5.1. Comiesięczne Raporty z Obsługi Incydentów

A. Najczęstszą praktyką jest przygotowywania comiesięcznych raportów z obsługi incydentów dla każdego klienta, zgodnie z warunkami umowy.

B. Comiesięczne raporty z obsługi incydentów zawierają informacje o wszystkich incydentach, które miały miejsce w danym okresie raportowania. Raporty obejmują szczegółowe informacje o rodzaju incydentu, priorytecie, działaniach podjętych w celu remediacji, statusie incydentu oraz analizie przyczyn.

C. Comiesięczne raporty są dostarczane klientowi w ustalonych terminach i formatach, zgodnie z umową.

5.2. Bieżące Raportowanie na Temat Stanu Bezpieczeństwa

A. Sprinttech SOC utrzymuje ścieżki eskalacji i konsultacji z klientami w celu bieżącego raportowania na temat stanu bezpieczeństwa. Klient może skorzystać z tych ścieżek, aby uzyskać informacje na temat bieżących incydentów, zagrożeń lub innych zdarzeń związanych z bezpieczeństwem informatycznym.

B. W ramach bieżącego raportowania na temat stanu bezpieczeństwa Sprinttech SOC udostępnia klientowi wszelkie dostępne informacje oraz rekomendacje dotyczące działań zaradczych.

5.3. Raportowanie Incydentów Krytycznych

A. Incydenty noszące znamiona krytyczne są raportowane klientowi w sposób natychmiastowy i priorytetowy.

B. Sprinttech SOC zapewnia pełne wsparcie klienta w obszarze prawnych aspektów incydentów krytycznych, w tym przygotowanie odpowiednich raportów i dokumentacji.

5.4. Audyt i Weryfikacja

A. Niniejsza polityka raportowania incydentów podlega okresowemu audytowi w celu zapewnienia jej skuteczności i zgodności z ustalonymi standardami.

B. Audyty są przeprowadzane przez wyznaczonego audytora wewnętrznego lub zewnętrznego.

6. Dostępność i zaufanie

6.1. Zapewnienie Dostępności Usług

A. Sprinttech zobowiązuje się do zapewnienia ciągłości działania swoich usług i systemów.

B. Odpowiednie środki techniczne i organizacyjne są wdrażane w celu minimalizacji zakłóceń w dostępie do usług oraz szybkiego przywracania działania w przypadku awarii.

6.2. Monitorowanie Dostępności

A. Dostępność usług jest regularnie monitorowana w celu wykrycia i rozwiązania potencjalnych problemów.

B. CSIRT Sprinttech podejmuje działania w celu zwiększenia dostępności w oparciu o wyniki monitoringu.

6.3. Planowanie Ciągłości Działania

A. Sprinttech przygotowuje i utrzymuje plan ciągłości działania, który określa procedury i środki w przypadku zakłóceń w dostępie do usług.

B. Plan ciągłości działania jest regularnie testowany i aktualizowany.

6.4. Zaufanie – Przestrzeganie Prawa

A. Sprinttech Sp z o.o. zobowiązuje się do przestrzegania wszelkich obowiązujących przepisów prawa związanych z bezpieczeństwem informacji, ochroną danych osobowych oraz innych regulacji branżowych.

B. Wszystkie działania podejmowane przez organizację muszą być zgodne z obowiązującym prawem, w tym przepisami dotyczącymi ochrony danych osobowych, prawa autorskiego, własności intelektualnej i innych.

6.5. Zaufanie – Etyka w przetwarzaniu informacji

A. Pracownicy Sprinttech są zobowiązani do przestrzegania najwyższych standardów etycznych w zakresie przetwarzania informacji. Wszelkie działania nieetyczne są surowo zabronione.

B. Organizacja promuje etyczne zachowanie wśród swojego personelu, partnerów biznesowych i dostawców.

6.6. Zaufanie – Ochrona Danych

A. Sprinttech zobowiązuje się do ochrony danych swoich klientów, partnerów oraz własnych informacji przed nieautoryzowanym dostępem, modyfikacją lub utratą.

B. Przetwarzanie danych osobowych odbywa się zgodnie z obowiązującymi przepisami dotyczącymi ochrony danych osobowych, w tym Rozporządzeniem Ogólnym o Ochronie Danych Osobowych (RODO) i innymi regulacjami krajowymi.

C. Wszelkie dane przechowywane są zgodnie z obowiązującymi przepisami i najlepszymi praktykami branżowymi.

D. Dane osobowe są przetwarzane wyłącznie na podstawie odpowiednich zgód lub zgodnie z innymi przepisami prawa.
E. Wszelkie zmiany w zakresie przetwarzania danych osobowych są uzgadniane z osobami, których dane dotyczą.
F. Wszelkie dane przetwarzane w systemach Sprinttech muszą być legalnie pozyskane i przetwarzane zgodnie z obowiązującym prawem.
G. Dostęp do danych jest ograniczony do osób, które są uprawnione do przetwarzania tych danych zgodnie z ich rolami i obowiązkami.

6.7. Zaufanie - Bezpieczeństwo Systemów

A. Sprinttech stosuje odpowiednie środki zabezpieczeń technicznych i organizacyjnych w celu ochrony danych oraz zapewnienia integralności i dostępności systemów informatycznych.
B. Regularne audyty bezpieczeństwa są przeprowadzane w celu identyfikacji słabości i wdrożenia środków zaradczych.

6.8. Zaufanie – Dostawcy

A. Organizacja współpracuje tylko z zaufanymi dostawcami, którzy również przestrzegają wysokich standardów bezpieczeństwa i poufności.

6.9. Zaufanie - Edukacja i Świadomość

A. Personel organizacji jest edukowany i świadomy znaczenia bezpieczeństwa informacji oraz roli każdego pracownika w jego zachowaniu.

6.10. Ciągłe Doskonalenie

A. Organizacja dąży do ciągłego doskonalenia swoich procesów związanych z dostępnością i zaufaniem.
B. Zmiany w politykach i procedurach są regularnie aktualizowane w celu dostosowania do zmieniających się zagrożeń i wymagań.

6.11. Audyty i Kontrole

A. Organizacja przeprowadza regularne audyty i kontrole, aby upewnić się, że zasady dostępności i zaufania są przestrzegane.
B. Wyniki audytów są analizowane, a wszelkie nieprawidłowości są korygowane.

7. Współpraca

Celem niniejszego punktu jest określenie zasad i wartości współpracy zarówno wewnętrznej, jak i zewnętrznej w kontekście bezpieczeństwa informacji i cyberbezpieczeństwa. Współpraca stanowi kluczowy element skutecznego zarządzania ryzykiem i ochroną informacji.

7.1. Współpraca - Działania Zespołu

- Personel Sprinttech jest zobowiązany do współpracy w zakresie realizacji celów bezpieczeństwa informacji i zapewnienia integralności systemów i danych.
- Sprinttech realizuje powyższe zobowiązanie poprzez cykliczne (dwa razy w tygodniu) spotkania całego zespołu specjalistów i kadry zarządzającej
- Współpracujący zespoły, takie jak zespół ds. bezpieczeństwa informatycznego, CSIRT (Computer Security Incident Response Team) oraz zespoły audytu i kontrolingu, współdziałają w celu osiągnięcia celów bezpieczeństwa.

7.2. Współpraca - Dzielenie Informacji

- Personel Sprinttech jest zachęcany do dzielenia informacji na temat zagrożeń i incydentów bezpieczeństwa wewnętrznie, co przyczynia się do skutecznego reagowania na incydenty.
- Personel Sprinttech realizuje współdzielenie wewnętrzne informacji poprzez wzajemny kontakt wielokanałowy, grupy zadaniowe oraz kontakt bezpośredni
- Współpraca międzydziałowa jest promowana w celu identyfikacji i rozwiązania potencjalnych problemów.

7.3. Współpraca Zewnętrzna

A. Partnerzy Biznesowi

- Sprinttech współpracuje z partnerami biznesowymi w celu zapewnienia bezpieczeństwa danych i informacji, a także w ramach wymiany informacji o zagrożeniach.
- Umowy z partnerami biznesowymi zawierają klauzule dotyczące bezpieczeństwa informacji i poufności danych.

B. Współpraca z Dostawcami

- Sprinttech współpracuje z dostawcami technologii i usług w celu zapewnienia zgodności z zasadami bezpieczeństwa informacji.
- Dostawcy są zobowiązani do przestrzegania wymagań bezpieczeństwa określonych w umowach.

C. Współpraca z Organizacjami Branżowymi

- Organizacja jest aktywnym uczestnikiem organizacji branżowych i inicjatyw mających na celu poprawę bezpieczeństwa informacji w danej branży.
- Współpraca z organizacjami branżowymi obejmuje udostępnianie informacji o zagrożeniach i udział w inicjatywach dotyczących bezpieczeństwa.

7.4. Współpraca w Ramach Rozwoju

- Personel jest zachęcany do uczestnictwa w szkoleniach, konferencjach i inicjatywach związanych z bezpieczeństwem informacji w celu zdobywania wiedzy i doświadczenia.
- Organizacja może wspierać rozwijanie umiejętności swojego personelu poprzez inwestycje w rozwój zawodowy.

8. Podsumowanie

Niniejszy dokument stanowi fundament naszej strategii bezpieczeństwa informacji oraz skupia się na kluczowych aspektach zapewnienia poufności, integralności i dostępności naszych oraz klientów danych i systemów. Jest to nie tylko dokument, ale także wyraz naszego zaangażowania w ochronę informacji i utrzymanie wysokich standardów bezpieczeństwa.

Polityka Organizacyjna Computer Security Incident Response Team Sprinttech, której treść została przedstawiona w tym dokumencie, ma kluczowe znaczenie dla organizacji w kontekście reagowania na incydenty. Oto kilka kluczowych kwestii, które warto podkreślić:

1. Ochrona Aktywów

Polityka ta ma na celu ochronę naszych aktywów informacyjnych, w tym danych klientów, własności intelektualnej i innych wartościowych informacji. Dzięki temu zapewniamy nie tylko naszym klientom, ale także sobie samym pewność, że ich informacje są bezpieczne i poufne.

2. Reagowanie na Incydenty

Polityka ta dostarcza wytycznych i procedur dotyczących reagowania na incydenty. Dzięki niej jesteśmy przygotowani na różnego rodzaju sytuacje kryzysowe i jesteśmy w stanie skutecznie zarządzać nimi, minimalizując potencjalne szkody.

3. Współpraca i Zaufanie

W polityce zawarte są zasady dotyczące współpracy zarówno wewnętrznej, jak i zewnętrznej. Współpraca ta pozwala nam budować zaufanie wobec partnerów biznesowych, dostawców i klientów.

4. Dostępność i Zaawansowane Technologie

Polityka bezpieczeństwa informacji promuje dostępność naszych usług i systemów. Jednocześnie zachęcamy do korzystania z najnowszych technologii, które pomagają nam utrzymać nasze środowisko informatyczne na najwyższym poziomie wydajności i bezpieczeństwa.

5. Prawo i Etyka

Podkreślamy znaczenie przestrzegania prawa i zasad etyki w kontekście przetwarzania informacji. Dla naszej organizacji ważne jest, aby działać zgodnie z obowiązującymi przepisami i promować etyczne zachowanie wśród pracowników.

Ten dokument stanowi wyraz naszego zobowiązania do ciągłego doskonalenia naszych praktyk bezpieczeństwa informacji i ochrony danych. Jest to dokument żywy, który będzie podlegał regularnym aktualizacjom, aby dostosować się do zmieniających się zagrożeń i wymagań.

Wszyscy pracownicy, partnerzy biznesowi i dostawcy są zachęcani do zapoznania się z treścią tej polityki i do jej przestrzegania. Bezpieczeństwo informacji to zadanie każdego z nas, i tylko wspólnymi siłami możemy osiągnąć sukces.

Dziękujemy za zaangażowanie i współpracę w zakresie wdrażania tej polityki. Razem tworzymy środowisko, w którym informacje są bezpieczne i organizacja jest odporna na zagrożenia.