DOKUMENTACJA BEZPIECZEŃSTWA I INTEGRALNOŚCI SIECI I USŁUG W TELEGO SP. Z O.O.

PREZES ZARZĄDU
Jacek Laskowski
30.12.2020

Telego Sp. z o.o. ul. Tadeusza Czackiego 7/9/11, 00-043 Warszawa,
NIP: 5213804216; REGON: 368855400; KRS 0000706498 Sąd Rejonowy w Warszawie XII Wydział Gospodarczy,
Kapitał zakładowy 9 505 000,00 zł w całości opłacony; Biuro Obsługi Klienta: 801 048 048, 29 765 06 50; www.telego.pl

Tabela zmian

Data	Autor	Zakres
30.12.2020	**Mariusz Kwiatkowski** **Kierownik Działu IT**	Utworzenie dokumentu

Aktualna wersja dokumentu publikowana jest w formie elektronicznej na portalu firmowym.

I. Cel dokumentacji

Celem niniejszego dokumentu jest wskazanie kluczowych elementów infrastruktury telekomunikacyjnej TeleGo Sp. z o.o. (dalej „TeleGo"), mających istotne znaczenie dla integralności sieci i działania usług telekomunikacyjnych, oraz wskazanie działań zabezpieczających ciągłość ich działania, zgodnie z rozporządzeniem Ministra Cyfryzacji z dnia 22 czerwca 2020 (Dz. U. z 2020 r., poz. 1130).

II. Właściciel dokumentacji, zasady aktualizacji i publikacji

Właścicielem niniejszej dokumentacji oraz Załączników jest **Kierownik Działu IT**. Właściciel odpowiedzialny jest za ich aktualizacje oraz publikowanie najświeższej wersji na portalu firmowym.

III. Kluczowe elementy infrastruktury telekomunikacyjnej TeleGo

Za kluczowe elementy infrastruktury telekomunikacyjnej TeleGo zapewniające ciągłość usług uznaje się:

1. Elementy infrastruktury i warstwy aplikacyjnej CRM, łącznie z modułami umożliwiającymi wymianę informacji z innymi operatorami/UKE (PLI CBD, moduł komunikacji z Polkomtelem) (zwanych dalej „CRM") (wyszególnione w załączniku 1);
2. Elementy infrastruktury i warstwy aplikacyjnej systemu doładowania kont w bazie PLK (zwanych dalej „SD") (wyszególnione w załączniku 2);
3. Elementy infrastruktury i warstwy aplikacyjnej call-center (zwanych dalej „CC") (wyszególnione w załączniku 3).

IV. Identyfikacja zagrożeń dla bezpieczeństwa i integralności usług

Poniższa tabela zawiera wykaz zidentyfikowanych zagrożeń dla bezpieczeństwa i integralności usług opartych o kluczową infrastrukturę telekomunikacyjną TeleGo.

lp.	Zagrożenie	Prawdopodobieństwo wystąpienia	Wpływ	Dotyczy systemów
1	Awaria elementów infrastruktury sprzętowej	niskie	średni	CRM SD CC
2	Awaria łączy internetowych od/do operatorów zewnętrznych	niskie	wysoki	SD
3	Awaria łączy internetowych u operatorów serwerowni	niskie	wysoki	CRM SD

				CC
4	Awaria łączy internetowych w siedzibie TeleGo i Ostrołęce	niskie	niski	CRM CC
5	Ataki na systemy informatyczne (sieciowe, aplikacyjne, fizyczne)	średnie	średni	CRM SD
6	Ataki hakerskie – próby nieuprawnionego dostępu do systemów	średnie	średni	CRM SD CC
7	Awarie elementów aplikacyjnych i systemowych (rozspójnienie baz danych, zawieszanie usług, błędy konfiguracyjne, brak miejsca na dyskach, etc.)	niskie	średni	CRM SD CC
8	Awarie w serwerowni (zasilania, klimatyzacji, itp.)	niskie	wysoki	CRM SD CC
9	Zdarzenia losowe w serwerowni (pożar, zalanie, włamanie itp.)	niskie	wysoki	CRM SD CC

V. Środki zapobiegawcze i minimalizujące skutki zagrożeń

Poniższa tabela zawiera wykaz zidentyfikowanych zagrożeń dla bezpieczeństwa i integralności usług opartych o kluczową infrastrukturę telekomunikacyjną TeleGo

lp.	Zagrożenie	Stosowane środki zapobiegawcze i minimalizujące skutki zagrożeń
1	Awaria elementów infrastruktury sprzętowej	• Redundancja kluczowych elementów infrastruktury sprzętowej • Umowy z dostawcami sprzętu oraz podwykonawcami odpowiedzialnymi za utrzymanie infrastruktury/systemów • Polityka backupów
2	Awaria łączy internetowych od/do operatorów zewnętrznych	• Redundancja kluczowych elementów infrastruktury sprzętowej
3	Awaria łączy internetowych u operatorów serwerowni	• Umowy z operatorami serwerowni zapewniającymi najwyższe standardy dostępu do sieci internetowej, posiadającymi odpowiednie zabezpieczenia przed awarią łączy
4	Awaria łączy internetowych w siedzibie TeleGo	• Umowy o dostawę łączy z wiodącymi operatorami na rynku telekomunikacyjnym • Awaryjne środki zapewniające łączność internetową w przypadku awarii • Wyposażenie pracowników w środki i sprzęt umożliwiające pracę zdalną i zarządzania systemami poza siedzibą TeleGo
5	Ataki na systemy informatyczne	• Monitoring elementów infrastruktury sprzętowej i sieciowej • Środki zabezpieczeń przed niepowołanymi próbami dostępu (firewall, tablice wykluczeń adresów IP) • Polityka zarządzania dostępem do systemów
6	Ataki hakerskie – próby nieuprawnionego dostępu do systemów	• Monitoring elementów infrastruktury sprzętowej i sieciowej

		• Środki zabezpieczeń przed niepowołanymi próbami dostępu (firewall, tablice wykluczeń adresów IP) • Polityka zarządzania dostępem do systemów
7	Awarie elementów aplikacyjnych i systemowych (rozspójnienie baz danych, zawieszanie usług, brak miejsca na dyskach, etc.)	• Redundancja kluczowych elementów systemów • Backupy, snapshoty • Instrukcje instalacji, konfiguracji i odtwarzania poszczególnych elementów systemu • Przechowywanie kodów źródłowych umożliwiających odtworzenie elementów systemu • Reagowanie na wykryte podatności, aktualizacje
8	Awarie w serwerowni	• Umowy z operatorami serwerowni zapewniającymi najwyższe standardy dostępu posiadającymi odpowiednie zabezpieczenia przed awariami prądu • Umowy z Ubezpieczycielami • UPS-y • Monitoring infrastruktury sprzętowej • Redundancja kluczowych elementów w serwerowni
9	Zdarzenia losowe w serwerowni	Backup offsite

VI. Zasady dostępu do kluczowej infrastruktury i przetwarzanych danych, zasady zdalnego przetwarzania danych, opis kluczowych środków zapobiegania ryzykom bezpieczeństwa stosowanych w TeleGo

Odpowiedzialność za kluczową infrastrukturę ponosi **Kierownik Działu IT**.

Systemy operacyjne komputerów:

- Konto ograniczone dla użytkowników (blokada instalowania oraz odinstalowywania oprogramowania);
- Konta systemowe zabezpieczone hasłem;
- Program antywirusowy ESET NOD32 Antivirus

a) Ochrona antywirusowa

b) Blokada za pomocą funkcji „kontroli korzystania z urządzeń" urządzeń zewnętrznych typu (Płyta CD/DVD, Pamięć masowa FireWire, Urządzenie Bluetooth, Urządzenie do tworzenia obrazów, Modem, Urządzenie przenośne);

- Blokowanie konta systemowego przy braku aktywności użytkownika przez 10 minut.

Serwerownia:

- Kontrola dostępu do pomieszczenia za pośrednictwem karty;
- Wydzielona strefa w systemie Alarmowym;
- Zasilanie awaryjne UPS podtrzymujący wszystkie urządzenia;
- System monitorujący temperaturę w pomieszczeniu;
- Zabezpieczenie antyprzepięciowe.

Budynek:

- Kontrola dostępu do budynku za pośrednictwem karty;
- Monitoring budynku przez agencję ochrony;
- Zabezpieczenia przeciwpożarowe zgodne z obowiązującymi standardami.

Oprogramowanie:

(systemy informatyczne dostępne są wyłącznie z wewnątrz sieci lokalnej lub za pośrednictwem VPN)

CRM

- Klucz aplikacji wymieniany przy aktualizacjach;
- Hasło wygasające po miesiącu w przypadku braku zmiany hasła blokowanie konta'
- Logi systemowe

Cloud

- wymiana informacji pomiędzy komputerami odbywa się za pośrednictwem prywatnej chmury dostępnej wyłącznie wewnątrz sieci'
- dostęp do informacji jest blokowany po osiągnięciu daty ważność ustawionej przy dodawaniu.

ESET Security Management Center

- wgląd w bezpieczeństwo stacjonarnych i zdalnych firmowych endpointów

Kopie bezpieczeństwa:

- Codziennie automatyczne kopie bezpieczeństwa baz danych przechowywane na oddzielnym urządzeniu'
- Kopie bezpieczeństwa wirtualnych maszyn'
- Kody źródłowe autorskiego oprogramowania spółki zabezpieczone są w repozytorium GitLab udostępnionym jedynie użytkownikom sieci lokalnej.

Poczta e-mail

- Wykorzystanie szyfrowanych protokołów komunikacji'
- Dodatkowe szyfrowanie załączników posiadających dane osobowe.

Instrukcje zarządzania systemem informatycznym:

- Zakaz podłączania własnego sprzętu teleinformatycznego do systemu informatycznego spółki oraz zakaz wykorzystywania systemów informatycznych dla celów innych niż związane z wykonywaniem obowiązków służbowych;
- Wymóg polityki bezpieczeństwa hasła (minimum 8 znaków, małe oraz wielkie litery, przynajmniej jena cyfra lub znak specjalny).

Firewall:

- Virtual Cluster 2 urządzenia;
- Dostęp do sieci z zewnątrz odbywa się za pośrednictwem IPsec VPN tunel'
- Polityki ograniczające ruch w sieci z wskazaniem odpowiednich adresów ip oraz portów. Użyte odpowiednie profile zabezpieczeń (Web Filter, AntiVirus, Application Control, IPS, PPX);
- Fragmentacja sieci wewnętrznej na vlan z ograniczeniem ruchu dostosowanym do rodzaju podłączonych urządzeń.

Przełączniki Switch:

- Przypisanie odpowiedniego vlan-u do konkretnego portu. Uniemożliwia to przełączenia podłączonego urządzenia do innej podsieci.

Monitoring stanu infrastruktury kluczowej prowadzony jest przy pomocy systemu PRTG oraz
FortiGate. System monitoringu pozwala na bieżące sprawdzanie zdefiniowanych parametrów komponentów systemów informatycznych na poziomie sieci, infrastruktury, systemu operacyjnego oraz aplikacji.

W przypadku wykrycia nieprawidłowości system monitoringu generuje alerty i wysyła je do administratorów systemów.

VII. Umowy z dostawcami zewnętrznymi kluczowe dla bezpieczeństwa infrastruktury

lp.	kontrahent	Umowa	zakres umowy	data obowiązywania
1	Wasko			
2	Orange			
3	T-mobile			
4	COIG			
5	Polkomtel			

Zawierając umowę mającą lub mogącą mieć wpływ na funkcjonowanie sieci lub usług należy zidentyfikować zagrożenia dla bezpieczeństwa sieci lub usług.

VIII. Audyty bezpieczeństwa

Audyt przeprowadza się:

1) co najmniej raz na dwa lata,
2) po każdym:

- stwierdzonym naruszeniu bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych o istotnym wpływie na funkcjonowanie sieci lub usług, w zakresie objętym naruszeniem, oraz
- wykryciu podatności zwiększającej poziom ryzyka wystąpienia naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych o istotnym wpływie na funkcjonowanie sieci lub usług, w zakresie objętym wykrytą podatnością.

IX. Wewnętrzna procedura zgłaszania naruszeń bezpieczeństwa lub integralności sieci lub usług oraz zasady informowania Prezesa UKE o naruszeniu bezpieczeństwa lub integralności sieci lub usług

Współpracownicy natychmiast zgłaszają **Kierownikowi Działu IT** wszelkie naruszenia lub próby naruszenia bezpieczeństwa lub integralności sieci lub usług.
W przypadku braku możliwości zgłoszenia **Kierownikowi Działu IT** zgłoszenia dokonuje osobie zastępującej, a w przypadku nieobecności tej osoby **Kierownik Działu Technicznego**.

Zgłoszenia dokonywane są w formie elektronicznej (adres e-mail) (a w przypadku braku możliwości przekazania w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji).

Zgłoszenia podlegają retencji, tak aby można było ustalić moment zgłoszenia.

W przypadku zgłoszonego przez współpracowników lub wykrytego naruszenia bezpieczeństwa lub integralności sieci lub usług **Kierownik Działu IT** (albo osoba zastępująca) informuje o tym niezwłocznie Zarząd Spółki.

Kierownik Działu IT (albo osoba zastępująca) oraz Zarząd Spółki dokonują kwalifikacji istotności wpływu na funkcjonowanie sieci lub usług, zgodnie z kryteriami określonymi w rozporządzeniu Ministra Cyfryzacji z dnia 20 września 2018 r. w sprawie kryteriów uznania naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług (Dz. U. z 2018 r., poz. 1830). W przypadku braku kontaktu z jedną z tych osób kwalifikacji dokonuje osoba, która jest dostępna.

1. Notyfikacja Prezesa UKE o naruszeniu bezpieczeństwa lub integralności sieci lub usług, które miało istotny wpływ na funkcjonowanie sieci lub usług

Jeżeli ustalono, że wpływ był istotny, **Kierownik Działu IT** (a w przypadku niedostępności, zastępca lub Zarząd Spółki) niezwłocznie informuje Prezesa UKE o naruszeniu bezpieczeństwa lub integralności sieci lub usług, które miało istotny wpływ na funkcjonowanie sieci lub usług, o podjętych działaniach zapobiegawczych i środkach naprawczych oraz podjętych przez przedsiębiorcę działaniach.

Wzór formularza stanowi Załącznik 4.

Informacja powinna być przesłana w formie elektronicznej z wykorzystaniem PUE, a w przypadku braku możliwości przekazania w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji.

2. Zasady działań i notyfikacja Prezesa UKE o zastosowanych środkach mających na celu zapewnienie bezpieczeństwa i integralności sieci, usług oraz przekazu komunikatów związanych ze świadczonymi usługami

Niezależnie od notyfikacji Prezesa UKE o naruszeniu bezpieczeństwa lub integralności sieci lub usług, które miało istotny wpływ na funkcjonowanie sieci lub usług, **Kierownik Działu IT** (albo osoba zastępująca) w porozumieniu z Zarządem Spółki podejmuje proporcjonalne i uzasadnione środki mające na celu zapewnienie bezpieczeństwa i integralności sieci, usług oraz przekazu komunikatów związanych ze świadczonymi usługami, w tym:

1) eliminację przekazu komunikatu, który zagraża bezpieczeństwu sieci lub usług;
2) przerwanie lub ograniczenie świadczenia usługi telekomunikacyjnej na zakończeniu sieci, z którego następuje wysyłanie komunikatów zagrażających bezpieczeństwu sieci lub usług.

Kierownik Działu IT (a w przypadku niedostępności, zastępca lub Zarząd Spółki) informuje Prezesa UKE niezwłocznie, o podjęciu takich środków, jednak nie później niż w ciągu 24 godzin od ich podjęcia.

W informacji zamieszcza się dane niezbędne do identyfikacji zagrożeń bezpieczeństwa sieci lub usług oraz przekazu komunikatów związanych ze świadczonymi usługami, ze wskazaniem podjętych środków naprawczych.

Informacja powinna być przesłana w formie elektronicznej z wykorzystaniem PUE, a w przypadku braku możliwości przekazania w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji.

X. Zgłaszanie przez użytkowników końcowych naruszeń bezpieczeństwa lub integralności sieci lub usług;

Spółka umożliwia użytkownikom końcowym dokonywanie zgłoszeń wszelkich naruszeń bezpieczeństwa lub integralności sieci lub usług przez Biuro Obsługi Klienta.

BOK niezwłocznie przekazuje zgłoszenie **Kierownikowi Działu IT** (albo osobie zastępującej).

Załącznik 1. Elementy infrastruktury kluczowej dla systemu CRM

A) Serwer DELL PowerEdge

- RAID z dyskami SATA SSD
- Podwójny nadmiarowy zasilacz (1+1)
- Dwuportowa karta LOM 1GbE

A) Serwer modułu PLI-CBD - DELL PowerEdge

- RAID z dyskami HDD SCSI
- Podwójny nadmiarowy zasilacz (1+1)

B) Serwer modułu do komunikacji z Polkomtelem (MVNE) - DELL PowerEdge

- RAID z dyskami HDD SCSI
- Podwójny nadmiarowy zasilacz (1+1)
- Dwuportowa karta 1GbE

B) Infrastruktura Sieciowa

- Przełączniki konfigurowalne CISCO Systems
- Firewall sprzętowy Fortigate

C) Połączenie VPN realizowane przez łącza internetowe.

- dwa niezależne łącza światłowodowe
- rodzaj połączenia (site-to-site)

D) Zabezpieczenie zasilania energetycznego

- rozdzielnia elektryczna
- System awaryjnego zasilania UPS Benning

Załącznik 2. Elementy infrastruktury kluczowej dla systemu SD

C) Serwer DELL PowerEdge

- RAID z dyskami HDD SCSI
- Podwójny nadmiarowy zasilacz (1+1)
- Dwuportowa karta 1GbE

D) Infrastruktura Sieciowa

- Przełączniki konfigurowalne CISCO Systems
- Firewall sprzętowy Fortigate

E) Połączenie VPN realizowane przez łącza internetowe.

- dwa niezależne łącza światłowodowe
- rodzaj połączenia (site-to-site)

F) Zabezpieczenia zasilania energetycznego

- rozdzielnia elektryczna
- System awaryjnego zasilania UPS Benning

Telego Sp. z o.o. ul. Tadeusza Czackiego 7/9/11, 00-043 Warszawa,
NIP: 5213804216; REGON: 368855400; KRS 0000706498 Sąd Rejonowy w Warszawie XII Wydział Gospodarczy,
Kapitał zakładowy 9 505 000,00 zł w całości opłacony; Biuro Obsługi Klienta: 801 048 048, 29 765 06 50; www.telego.pl

Załącznik 3. Elementy infrastruktury kluczowej dla systemu CC

A) Zestaw dwóch Serwerów HP ProLiant

- RAID z dyskami HP SAS
- Podwójny nadmiarowy zasilacz (1+1)
- Dwuportowa karta LOM 1GbE

B) Infrastruktura Sieciowa

- Przełączniki konfigurowalne CISCO Systems
- Firewall sprzętowy Fortigate

C) Trakty telekomunikacyjne

- zestaw kanałów E1 przesyłanych poprzez dwa niezależne łącza światłowodowe

D) Zabezpieczenia zasilania energetycznego

- rozdzielnia elektryczna
- System awaryjnego zasilania UPS Benning

Telego Sp. z o.o. ul. Tadeusza Czackiego 7/9/11, 00-043 Warszawa,
NIP: 5213804216; REGON: 368855400; KRS 0000706498 Sąd Rejonowy w Warszawie XII Wydział Gospodarczy,
Kapitał zakładowy 9 505 000,00 zł w całości opłacony; Biuro Obsługi Klienta: 801 048 048, 29 765 06 50; www.telego.pl

Załącznik 4. Wzór formularza do przekazywania Prezesowi UKE informacji o naruszeniu bezpieczeństwa lub integralności sieci lub usług, które miało istotny wpływ na funkcjonowanie sieci lub usług, o podjętych działaniach zapobiegawczych i środkach naprawczych oraz podjętych przez przedsiębiorcę działaniach

FORMULARZ INFORMACJI O NARUSZENIU BEZPIECZEŃSTWA LUB INTEGRALNOŚCI SIECI LUB USŁUG TELEKOMUNIKACYJNYCH, KTÓRE MIAŁO ISTOTNY WPŁYW NA FUNKCJONOWANIE SIECI LUB USŁUG	
I. Dane przedsiębiorcy telekomunikacyjnego	
1. Firma przedsiębiorcy lub nazwa innego podmiotu uprawnionego do wykonywania działalności gospodarczej na podstawie odrębnych przepisów	
2. Numer w rejestrze przedsiębiorców telekomunikacyjnych	
3. Siedziba i adres przedsiębiorcy	
II. Dane osoby składającej zgłoszenie	
1. Imię i nazwisko	
2. Nr telefonu służbowego	
3. E-mail służbowy	
III. Dane kontaktowe osoby uprawnionej do składania Prezesowi Urzędu Komunikacji Elektronicznej wyjaśnień dotyczących zgłaszanych informacji	
1. Imię i nazwisko	
2. Nr telefonu służbowego	
3. E-mail służbowy	
IV. Opis wpływu naruszenia na usługi i informacje o przyczynie naruszenia	
1. Usługi, **na które naruszenie wywarło wpływ (należy zaznaczyć odpowiednio jedną lub kilka)**	
a) publicznie dostępna usługa telefoniczna świadczona w stacjonarnej publicznej sieci telekomunikacyjnej Należy wskazać technologię lub standard (np. PSTN, DSL, VoIP, światłowód)	☐
b) publicznie dostępna usługa telefoniczna świadczona w ruchomej publicznej sieci telekomunikacyjnej Należy wskazać technologię lub standard (np. GSM, UMTS, LTE)	☐
c) usługa dostępu do sieci Internet świadczona w stacjonarnej publicznej sieci telekomunikacyjnej Należy wskazać technologię lub standard (np. DSL, światłowód, HFC)	☐
d) usługa dostępu do sieci Internet świadczona w ruchomej publicznej sieci telekomunikacyjnej Należy wskazać technologię lub standard (np. GPRS/EDGE, UMTS, LTE)	☐
e) SMS	☐
f) MMS	☐
g) rozpowszechnianie lub rozprowadzanie programów radiowych lub telewizyjnych drogą satelitarną	☐
h) rozpowszechnianie lub rozprowadzanie programów radiowych lub telewizyjnych w sieciach kablowych	☐

i) rozpowszechnianie lub rozprowadzanie programów radiowych lub telewizyjnych naziemnie ☐
2. Elementy **infrastruktury, na które naruszenie wywarło wpływ (należy zaznaczyć odpowiednio jedną pozycję lub kilka)**
☐ stacje bazowe i kontrolery (np. BTS, NodeB, RNC)
☐ elementy komutujące sieci (np. MSC, VLR, SGSN, GGSN)
☐ rejestry użytkowników lub lokalizacji (np. HLR, HSS, AuC)
☐ przełączniki sieciowe (np. local Exchanges, routery, DSLAM)
☐ węzły transmisyjne (np. SDH, WDM)
☐ sieć rdzeniowa (np. światłowodowa, kable miedziane)
☐ punkty styku sieci lub wymiany ruchu internetowego (np. IXP, IP transit)
☐ rejestry domen najwyższego poziomu (TLD)
☐ serwery DNS
☐ system zasilania (np. transformatory, wysokie napięcie)
☐ systemy podtrzymania (np. generatory, akumulatory)
☐ inne (należy wymienić jakie) .....
3. Informacje **o wpływie naruszenia**
a) liczba użytkowników danego przedsiębiorcy, na których naruszenie miało wpływ, według wyliczeń przedsiębiorcy (należy wskazać liczbę użytkowników, którzy w konsekwencji naruszenia zostali pozbawieni możliwości korzystania z usług, w tym wykonywania połączeń z numerami alarmowymi – odrębnie dla każdej z usług wskazanej przez przedsiębiorcę w części IV pkt 1)
b) wartość procentowa z ogólnej liczby użytkowników danego przedsiębiorcy, jaką stanowią użytkownicy danej usługi, na których naruszenie wywarło wpływ, według wyliczeń przedsiębiorcy – odrębnie dla każdej z usług wskazanej przez przedsiębiorcę w części IV pkt 1
c) czas trwania niedostępności usług lub ograniczenia dostępności usług telekomunikacyjnych (należy wskazać moment rozpoczęcia i zakończenia niedostępności lub ograniczenia dostępności usług telekomunikacyjnych w formacie RRRR-MM-DD, GG:MM)
d) obszar, na którym wystąpiło naruszenie
e) wpływ naruszenia na połączenia z numerami alarmowymi
f) wpływ naruszenia na poziom ochrony tajemnicy telekomunikacyjnej
g) wpływ naruszenia na możliwość realizacji zadań lub obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego
h) inne informacje o wpływie naruszenia (bez danych osobowych)
4. Informacje **o przyczynie naruszenia**
Kategoria naruszenia (należy zaznaczyć odpowiednio jedną lub kilka)
a) klęska żywiołowa/katastrofa ☐
.....
b) błąd ludzki ☐
.....
c) atak na infrastrukturę lub usługi ☐
.....
d) awaria sprzętu lub oprogramowania ☐

.....

e) awaria po stronie podmiotu trzeciego lub współpracującego ☐

.....

f) inna (należy wskazać jaka) ..... ☐

Przyczyny naruszenia (należy zaznaczyć odpowiednio jedną lub kilka)

☐ przecięcie kabli

☐ kradzież kabli

☐ powódź

☐ opady śniegu

☐ burza

☐ przerwa w zasilaniu

☐ przepięcie

☐ atak fizyczny

☐ cyberatak

☐ źle wprowadzone modyfikacje

☐ złe utrzymanie urządzeń

☐ przeciążenie sieci

☐ brak paliwa

☐ awaria sprzętu

☐ błąd oprogramowania

☐ wada procedury

☐ inna (należy podać jaka) .....

V. Szczegółowe informacje o naruszeniu

1. Opis naruszenia wraz z wyszczególnieniem bezpośrednich przyczyn jego powstania:

a) opis naruszenia

b) informacja o urządzeniach, systemach, aplikacjach etc., które spowodowały naruszenie (w szczególności: nazwa, dane modelu, producent, podstawowe dane techniczne, funkcje etc.)

c) informacja o wypełnieniu wymaganych warunków pracy urządzeń, systemów, aplikacji etc., które spowodowały naruszenie (w szczególności dotyczących: warunków atmosferycznych, zasilania, dostępu osób trzecich, spełniania wymagań eksploatacyjnych producenta etc.)

2. Informacje o podjętych działaniach zapobiegawczych

3. Informacje o podjętych środkach naprawczych

4. Informacja o podjętych działaniach, o których mowa w art. 175 i art. 175c ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne

5. Informacja o wpływie naruszenia na infrastrukturę lub usługi innych przedsiębiorców telekomunikacyjnych

VI. Wnioski i inne dodatkowe informacje