ZASADY BIZNESOWE DOTYCZĄCE BEZPIECZNEGO POSTĘPOWANIA Z INFORMACJAMI

Cel: Kluczowe komunikaty dotyczące postępowania z informacjami pochodzącymi od firmy Lilly lub przekazanymi w jej imieniu, zwane dalej Informacjami.

Dlaczego jest to ważne?

- Twoja organizacja i jej pracownicy są cenionymi współpracownikami firmy Lilly, a działania podejmowane przez Ciebie i Twoich pracowników są częścią pierwszej i najlepszej linii obrony przed naruszeniem Informacji.
- Ochrona informacji ma zasadnicze znaczenie dla firmy Lilly i pacjentów, którym świadczymy usługi.

Poniższe kluczowe komunikaty, oparte na najlepszych praktykach branżowych, w tym w ramach NIST Cybersecurity Framework, należy uwzględnić w obecnych praktykach, aby nadal zmniejszać ryzyko podczas przetwarzania Informacji.

Ogólnie:

- Unikaj tworzenia duplikatów elektronicznych lub papierowych kopii dokumentów zawierających Informacje, chyba że jest to absolutnie konieczne.

Elektroniczne przechowywanie danych:

- Pliki elektroniczne zawierające Informacje muszą być bezpiecznie przechowywane. Wymienne urządzenia przechowujące dane, takie jak zewnętrzne dyski twarde i USB, nie mogą być używane bez zgody firmy Lilly.
    - Przy przyznawaniu dostępu do plików należy stosować zasadę najmniejszego przywileju (tj. dostęp do Informacji powinien być przyznawany tylko tym, którzy muszą wiedzieć, nie więcej niż jest to potrzebne i tylko na wymagany okres). Dostęp należy zweryfikować proporcjonalnie do poziomu wrażliwości danych. Obejmuje to lokalizacje magazynowe, którymi zarządzasz, a także te zarządzane przez podwykonawców.
    - Terminowa dezaktywacja dostępu powinna nastąpić po wyjściu z firmy lub gdy osoby fizyczne nie mają już biznesowej potrzeby dostępu do Informacji.
- Informacje NIE mogą być przechowywane w następujących lokalizacjach bez zgody firmy Lilly:
    - na urządzeniach osobistych pracowników, takich jak laptopy, iPady itp.
    - na zewnętrznych usługach lub witrynach pamięci masowej.

Elektroniczny transfer danych:

- Pliki elektroniczne zawierające Informacje muszą być bezpiecznie przekazywane. Skonsultuj się z osobą kontaktową w firmie Lilly, aby ustalić preferowaną metodę przekazywania informacji. Wymienne urządzenia przechowujące dane, takie jak zewnętrzne dyski twarde, płyty CD/DVD i USB, nie mogą być używane bez zgody firmy Lilly.
- Informacji NIE WOLNO przekazywać za pośrednictwem:
    - niezabezpieczonych wiadomości e-mail (chyba że poziom wrażliwości danych nie wymaga takiej gwarancji);
    - zewnętrznych urządzeń przechowujących dane, takich jak zewnętrzny dysk twardy lub USB (bez zgody firmy Lilly);
    - osobistych wiadomości e-mail;

Telekonferencje/spotkania online:

- Skorzystaj z usług zatwierdzonych przez firmę Lilly do planowania i prowadzenia spotkań dotyczących działalności firmy. W przypadku pytań dotyczących telekonferencji/spotkań online skonsultuj się z osobą kontaktową firmy Lilly.
- Bądź świadomy swojego otoczenia i zachowaj ostrożność podczas omawiania Informacji.

Bezpieczeństwo fizyczne:

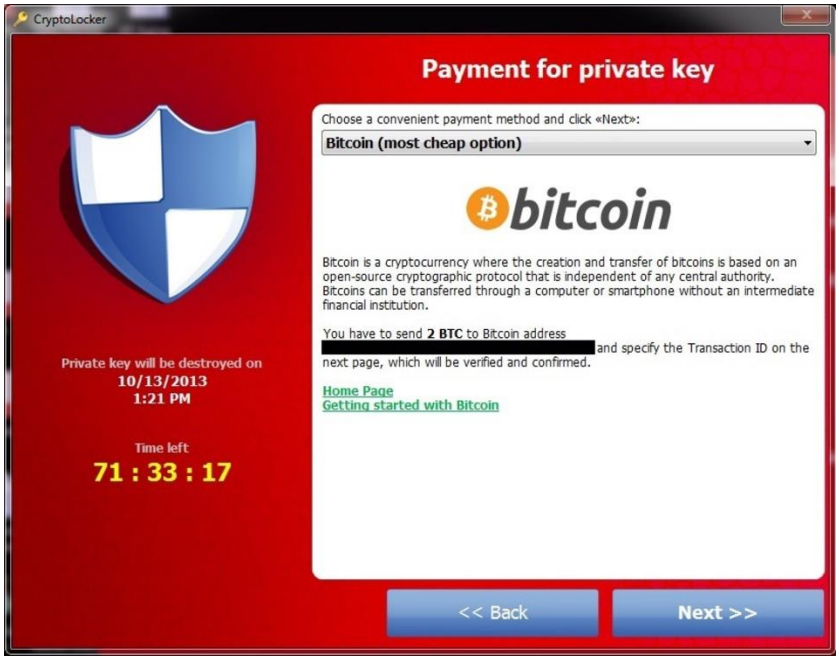
- Utrzymuj bezpieczne miejsce pracy:
  - zablokuj dostęp do swoich urządzeń za KAŻDYM razem, gdy od nich odejdziesz;
  - urządzenia należy umieścić w zamykanej szafce, zamknąć lub zabrać ze sobą, gdy wyjeżdżasz na cały dzień, wyjeżdżasz w podróż służbową lub na wakacje;
  - zamknij biurko, szafki i szafkę/biuro, gdy wychodzisz na cały dzień, jesteś w podróży służbowej lub na wakacjach;
  - nie zostawiaj wydruków w drukarkach;
  - wyrzucanie Informacji w bezpieczny sposób (np. niszczenie);

Wiadomości błyskawiczne i wiadomości tekstowe:

- Skorzystaj z narzędzia zatwierdzonego przez firmę Lilly do obsługi wiadomości błyskawicznych i wiadomości tekstowych dla firm. Skonsultuj się z osobą kontaktową firmy Lilly, jeśli masz pytania związane z wiadomościami błyskawicznymi lub wiadomościami tekstowymi.

Zgłaszanie incydentów związanych z bezpieczeństwem Informacji:

- Zgłaszaj incydenty osobie kontaktowej z firmy Lilly w odpowiednim czasie. Incydenty obejmują między innymi:
  - wiadomość e-mail zawierająca informacje została przypadkowo wysłana do niezamierzonego odbiorcy;
  - zgubiony lub skradziony laptop, dysk twardy lub przenośny nośnik danych zawierający Informacje;
  - podwykonawca mający dostęp do Informacji zgłasza zdarzenie Twojej firmie;
  - otrzymanie ransomware, rodzaju złośliwego oprogramowania zaprojektowanego do blokowania dostępu do urządzenia do momentu zapłacenia określonej kwoty. Zobacz przykład poniżej. Natychmiastowe wykonanie poniższych czynności może pomóc zmniejszyć ryzyko:
    - odłącz kabel sieciowy lub wyłącz kartę sieci bezprzewodowej;
    - hibernuj urządzenie;



Uważaj na inżynierię społeczną *(np. phishing, vishing, SMiShing)*!:

- Inżynieria społeczna to oszustwo mające na celu nakłonienie osób do ujawnienia informacji poufnych lub osobistych, które mogą zostać wykorzystane do nieuczciwych celów. Oszuści podszywają się pod wiarygodne źródło, próbując ukraść tożsamość lub odzyskać informacje, takie jak hasła, dane bankowe i numery kart kredytowych itp.

- **Phishing** (e-mail)
  - Phishing to próba wyłudzenia informacji poprzez nieoczekiwaną wiadomość, a jej cechy obejmują:
    - alarmujące wezwanie do działania (na przykład spóźniona płatność kartą kredytową);
    - element czasu (na przykład termin płatności przypada w ciągu dwóch dni);
    - konsekwencja (na przykład rozwiąż ten problem lub stanie się coś złego);
    - słaba gramatyka lub błędna pisownia słów;
    - ORAZ zawsze ma coś do „kliknięcia”, na przykład łącze lub załącznik
  - Kliknięcie nieznanego załącznika lub łącza w wiadomości e-mail może spowodować zagrożenie dla komputera i całej sieci.

- **Vishing** (rozmowy telefoniczne lub wiadomości głosowe)
  - Vishing to próba wyłudzenia informacji (phishing głosowy) poprzez nieoczekiwaną rozmowę telefoniczną:
    - podczas której szuka się potwierdzenia informacji lub żąda informacji;
    - która może być używana w połączeniu z atakiem typu phishing;
- **SMiShing** (wiadomości tekstowe SMS)
  - to próba wyłudzenia informacji poprzez nieoczekiwaną wiadomość tekstową, która:
    - podczas której szuka się potwierdzenia informacji lub żąda informacji;
    - która może być używana w połączeniu z atakiem typu phishing;
    - zazwyczaj zawiera coś, co można „kliknąć”, na przykład łącze lub załącznik;

- **Jeśli masz adres e-mail firmy Lilly**, weźmiesz udział w formalnym programie szkoleniowym firmy Lilly dotyczącym phishingu.
  - Osoby, które wielokrotnie klikają w nieautoryzowane łącza, zostaną zgłoszone firmie zewnętrznej z oczekiwaniem na kontynuację szkolenia. Skonsultuj się z osobą kontaktową firmy Lilly, jeśli masz pytania dotyczące formalnego programu szkoleniowego firmy Lily dotyczącego phishingu.
  - Jeśli korzystasz z konta e-mail firmy Lilly o365, zgłaszaj podejrzane wiadomości e-mail za pomocą przycisku „Report Phishing” (Zgłoś phishing) na wstążce „Home” (Strona główna) programu Outlook.

  - Jeśli jesteś połączony z siecią wewnętrzną Lilly przez VPN lub virtual.lilly.com, zgłaszaj podejrzaną wiadomość przez cyber@lilly.com.

- **Wstrzymaj i sprawdź. Użyj swojej intuicji:**
  - Jeśli wiadomość e-mail wydaje się podejrzana, poświęć chwilę, aby dokładnie się jej przyjrzeć.
  - Nie klikaj łączy ani nie otwieraj załączników, jeśli się ich nie spodziewasz.
  - Jeśli nie masz adresu e-mail firmy Lilly i klikniesz łącze lub otworzysz załącznik w wiadomości, którą uważasz za podejrzaną, zgłoś to za pośrednictwem procesu pracodawcy.

Jeśli masz pytania lub wątpliwości:

- Skonsultuj się z osobą kontaktową firmy Lilly, jeśli masz pytania lub wątpliwości związane z którymkolwiek z omówionych powyżej elementów.
- Te informacje są również dostępne w witrynie Supplier Portal (Portal dostawców) w ramach Operating Responsibility (Odpowiedzialności operacyjnej) w Supplier Resources (Zasobach dostawcy).