UNTERNEHMENSVORSCHRIFTEN FÜR DEN SICHEREN UMGANG MIT INFORMATIONEN

Zweck: Schlüsselbotschaften für den Umgang mit Informationen im Eigentum von Lilly oder die im Auftrag von Lilly bereitgestellt werden, im Folgenden als Informationen bezeichnet.

Warum ist das wichtig?

- Ihre Organisation und Ihre Mitarbeiter leisten einen wertvollen Beitrag für Lilly, und Maßnahmen, die Sie und Ihre Mitarbeiter ergreifen, sind Teil der ersten und besten Line of Defense für Informationsmissbrauch.
- Der Schutz von Informationen ist für Lilly und die Patienten, denen wir dienen, von wesentlicher Bedeutung.

Die folgenden Schlüsselbotschaften, die auf branchenüblichen Best Practices basieren, einschließlich des NIST Cybersecurity Framework, sollten in die derzeit angewendeten Praktiken aufgenommen werden, um das Risiko beim Umgang mit Informationen weiter zu verringern.

Im Allgemeinen:

- Vermeiden Sie doppelte elektronische oder ausgedruckte Kopien von Dokumenten, die Informationen enthalten, es sei denn, diese sind unbedingt erforderlich.

Elektronische Datenspeicherung:

- Elektronische Dateien, die Informationen enthalten, müssen sicher gespeichert werden. Wechselmedien wie externe Festplatten und USB-Sticks dürfen ohne Genehmigung von Lilly nicht verwendet werden.
    - Das Prinzip der geringsten Rechte sollte bei der Gewährung von Zugriff auf Dateien angewendet werden (d. h., der Zugriff auf Informationen sollte nur Personen gewährt werden, die ihn unbedingt benötigen, es sollten nicht mehr Rechte als erforderlich und nur für die erforderliche Zeit gewährt werden). Der Zugriff sollte entsprechend der Vertraulichkeitsstufe überprüft werden. Dies umfasst sowohl von Ihnen als auch von Ihren Subunternehmern verwaltete Speicherorte.
    - Die rechtzeitige Deaktivierung des Zugriffs sollte nach dem Ausscheiden aus dem Unternehmen erfolgen oder wenn Einzelpersonen keinen geschäftlichen Grund mehr haben, auf Informationen zuzugreifen.
- Informationen dürfen ohne Genehmigung von Lilly NICHT an folgenden Orten gespeichert werden:
    - Persönliche Geräte der Mitarbeiter, wie z. B. Laptops, iPads usw.
    - Externe Speicherdienste oder -orte.

Elektronische Datenübertragung:

- Elektronische Dateien, die Informationen enthalten, müssen auf sichere Weise übertragen werden. Wenden Sie sich an Ihren Lilly-Ansprechpartner, um die bevorzugte Methode für die Informationsübertragung zu ermitteln. Wechselmedien wie externe Festplatten, CDs/DVDs und USB-Sticks dürfen ohne Genehmigung von Lilly nicht verwendet werden.
- Informationen dürfen NICHT übertragen werden über:
    - Ungesicherte E-Mails (es sei denn, die Vertraulichkeitsstufe steht dem nicht entgegen).
    - Externe Speichergeräte wie externe Festplatten oder USB-Sticks (ohne Genehmigung von Lilly).
    - Persönliche E-Mails.

Telefonkonferenzen/Online-Meetings:

- Verwenden Sie von Lilly genehmigte Besprechungsdienste, um Besprechungen über die Unternehmensgeschäfte zu planen und durchzuführen. Wenden Sie sich an Ihren Lilly-Ansprechpartner, wenn Sie Fragen zu Telefonkonferenzen/Online-Meetings haben.
- Achten Sie auf Ihre Umgebung und seien Sie vorsichtig, wenn Sie Informationen besprechen.

Physische Sicherheit:

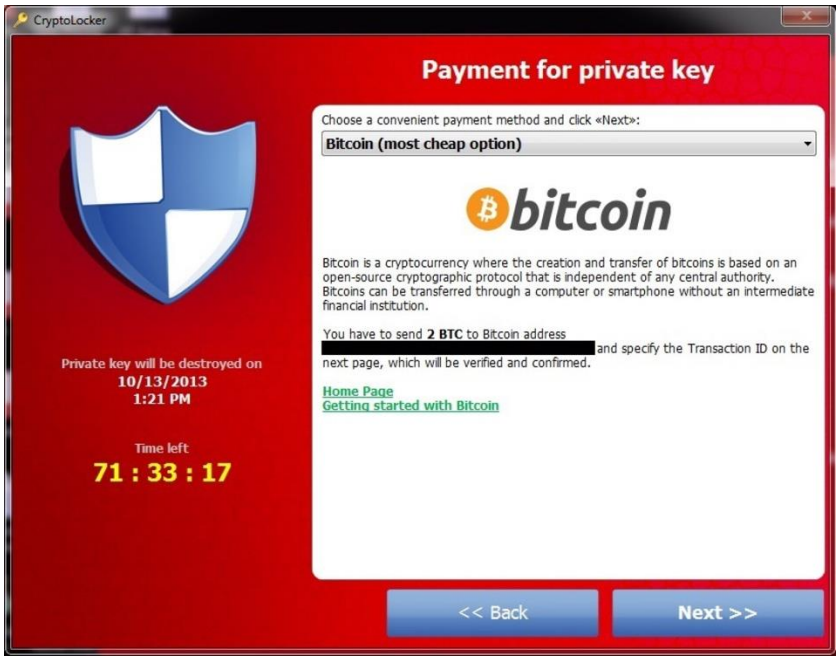
- Wahrung eines sicheren Arbeitsbereichs:
    - Sperren Sie den Zugriff auf Ihre Geräte IMMER, wenn Sie sich von ihnen entfernen.
    - Geräte sollten in einem abschließbaren Schrank aufbewahrt, mit einem Kabelschloss verschlossen oder mitgenommen werden, wenn Sie Feierabend machen, geschäftlich unterwegs sind oder in Urlaub gehen.
    - Schließen Sie Ihren Schreibtisch, Ihre Schränke und Ihr Schließfach/Büro ab, wenn Sie Feierabend machen, geschäftlich unterwegs sind oder in Urlaub gehen.
    - Lassen Sie keine Ausdrucke im Drucker liegen.
    - Entsorgen Sie Informationen unter Wahrung der Vertraulichkeit (z. B. Schreddern).

Sofort- und Textnachrichten:

- Verwenden Sie ein von Lilly genehmigtes Tool für Sofort- und Textnachrichten im Zusammenhang mit den Unternehmensgeschäften. Wenden Sie sich an Ihren Lilly-Ansprechpartner, wenn Sie Fragen zu Sofort- oder Textnachrichten haben.

Meldung von Vorfällen im Bereich der Informationssicherheit:

- Melden Sie Vorfälle rechtzeitig Ihrem Lilly-Ansprechpartner. Beispiele für Vorfälle sind insbesondere:
    - E-Mails mit Informationen wurden versehentlich an einen unbeabsichtigten Empfänger gesendet.
    - Verlorener oder gestohlener Laptop, Festplatte oder Wechseldatenträger mit Informationen darauf.
    - Ein Subunternehmer mit Zugriff auf Informationen weist Ihr Unternehmen auf einen Vorfall hin.
    - Erhalt von Ransomware, eine Art schädlicher Software, die den Zugriff auf das Gerät blockiert, bis eine bestimmte Summe gezahlt wird. Siehe das Beispiel im Anschluss. Das sofortige Ausführen der folgenden Schritte kann zur Risikominderung beitragen:
        - Ziehen Sie das Netzwerkkabel vom Gerät oder deaktivieren Sie den WLAN-Adapter.
        - Versetzen Sie das Gerät in den Ruhezustand.



Vorsicht vor Social Engineering *(z. B. Phishing, Vishing, SMiShing)***:**

- Social Engineering bezeichnet Täuschungsmanöver, um Personen dazu zu bewegen, vertrauliche oder persönliche Informationen preiszugeben, die für betrügerische Zwecke verwendet werden können. Betrüger tarnen sich als seriöse Quelle, um Identitäten zu stehlen oder Informationen wie Passwörter, Bankdaten, Kreditkartennummern usw. abzurufen.
    - **Phishing** (E-Mail)
        - Ein Phishing-Versuch ist eine unerwartete Nachricht, deren Merkmale unter anderem folgende sind:
            - Ein alarmierender Aufruf zum Handeln (z. B. verspätete Kreditkartenzahlung).
            - Ein Zeitelement (zum Beispiel ist etwas innerhalb von zwei Tagen fällig).
            - Eine Konsequenz (zum Beispiel, lösen Sie dieses Problem, oder Ihnen passiert etwas Schlimmes).
            - Schlechte Grammatik oder falsch geschriebene Wörter.
            - UND die Nachricht beinhaltet immer ein Element zum darauf „Klicken“, wie einen Link oder Anhang
        - Wenn Sie in einer E-Mail auf einen unbekannten Anhang oder Link klicken, können Ihr Computer und das gesamte Netzwerk gefährdet sein.

    - **Vishing** (Telefonanrufe oder Sprachnachrichten)
        - Ein Vishing-Versuch (Voice Phishing) ist ein unerwarteter Anruf:
            - Mit dem die Bestätigung von Informationen erzielt werden soll oder Informationen angefordert werden sollen.
            - Der in Kombination mit einem Phishing-Angriff verwendet werden kann.
    - **SMiShing** (SMS-Textnachrichten)
        - Ein SMiShing-Versuch ist eine unerwartete Textnachricht, die:
            - Mit dem die Bestätigung von Informationen erzielt werden soll oder Informationen angefordert werden sollen.
            - Der in Kombination mit einem Phishing-Angriff verwendet werden kann.
            - Normalerweise ein Element zum darauf „Klicken“ enthält, wie einen Link oder Anhang.

- **Wenn Sie eine Lilly-E-Mail-Adresse haben**, nehmen Sie am formellen Programm zur Aufklärung in Bezug auf Phishing von Lilly teil.
    - Personen, die Wiederholungsklicker sind, werden an Dritte gemeldet, damit sie ein Follow-up-Coaching erhalten können. Wenden Sie sich an Ihren Lilly-Ansprechpartner, wenn Sie Fragen zum formellen Programm zur Aufklärung in Bezug auf Phishing von Lilly haben.
    - Wenn Sie ein Lilly o365-E-Mail-Konto verwenden, melden Sie verdächtige E-Mails über die Schaltfläche Report Phishing (Phishing melden) im Outlook-Menüband der Registerkarte Home (Start).

    - Wenn Sie über VPN oder virtual.lilly.com mit dem internen Lilly-Netzwerk verbunden sind, melden Sie verdächtige Nachrichten über cyber@lilly.com.

- **Machen Sie Pause und untersuchen Sie die E-Mail. Verlassen Sie sich auf Ihre Intuition:**
    - Wenn eine E-Mail verdächtig erscheint, nehmen Sie sich einen Moment Zeit, um sich die Nachricht genau anzusehen.
    - Klicken Sie nicht auf Links oder öffnen Sie keine Anhänge, wenn Sie diese nicht erwartet haben.

- Wenn Sie keine Lilly-E-Mail-Adresse haben und auf einen Link klicken oder einen Anhang in einer Nachricht öffnen, die Sie für verdächtig halten, melden Sie dies bitte über den Prozess Ihres Arbeitgebers.

Wenn Sie Fragen oder Bedenken haben:

- Wenden Sie sich an Ihren Lilly-Ansprechpartner, wenn Sie Fragen oder Bedenken in Bezug auf die oben genannten Punkte haben.
- Diese Informationen finden Sie auch im Supplier Portal (Lieferantenportal) unter „Operating Responsibility in the Supplier Resources“ (Betriebsverantwortung bei den Lieferantenressourcen).