Inhalt

Gesetze

NIS

Das NIS steht für "Netzwerk- und Informationssystemsicherheit" und ist ein EU-weites Gesetzgebungsinstrument, das Mindestsicherheitsanforderungen für Netzwerk- und Informationssysteme festlegt. Das Ziel des NIS ist es, die Sicherheit von Informationstechnologie-Systemen in wichtigen Sektoren wie Energie, Verkehr, Bankwesen, Gesundheitswesen und Kommunikation zu gewährleisten.

Das NIS beinhaltet die Verpflichtung der Mitgliedstaaten der EU, nationale Strategien und Richtlinien zur Verbesserung der Cybersicherheit zu entwickeln. Es legt auch Mindestanforderungen für den Schutz von kritischen Infrastrukturen und digitalen Diensten fest. Dazu gehören unter anderem:

- Die Identifizierung von Risiken und Bedrohungen für die Cybersicherheit
- Die Umsetzung von Sicherheitsmaßnahmen und Standards
- Die Meldung von Sicherheitsvorfällen an nationale Behörden
- Die Zusammenarbeit zwischen den Mitgliedstaaten und der Europäischen Union im Falle von Cyberangriffen
- Die Ernennung nationaler Behörden und CSIRTs (Computer Security Incident Response Teams), die für die Aufrechterhaltung der Cybersicherheit zuständig sind

Das NIS hat das Ziel, die Resilienz und Robustheit von Informationssystemen in der EU zu stärken und die Fähigkeit der Mitgliedstaaten zu verbessern, auf Cyberangriffe zu reagieren und darauf zu reagieren.

DSGVO

Die Datenschutz-Grundverordnung (DSGVO) ist ein europäisches Datenschutzgesetz, das im Mai 2018 in der gesamten EU in Kraft getreten ist. Sie regelt den Schutz personenbezogener Daten und gibt den Betroffenen mehr Kontrolle über ihre Daten. Im Wesentlichen zielt die DSGVO darauf ab, das Recht auf Datenschutz in der gesamten Europäischen Union zu stärken und zu vereinheitlichen.

Die DSGVO stellt sicher, dass Unternehmen und Organisationen verantwortungsbewusst mit personenbezogenen Daten umgehen. Sie verpflichtet Unternehmen und Organisationen, die personenbezogene Daten verarbeiten, die notwendigen technischen und organisatorischen Maßnahmen zu ergreifen, um sicherzustellen, dass diese Daten sicher sind.

Ein wichtiger Aspekt der DSGVO ist die Einwilligung der betroffenen Person. Unternehmen müssen die Einwilligung der betroffenen Person einholen, bevor sie personenbezogene Daten erheben, verarbeiten oder nutzen dürfen. Diese Einwilligung muss freiwillig und informiert erfolgen. Die betroffene Person muss über die Art der erhobenen Daten, den Zweck der Verarbeitung und die Identität des Datenverantwortlichen informiert werden.

Die DSGVO gibt den betroffenen Personen auch das Recht, ihre personenbezogenen Daten einzusehen, zu korrigieren oder zu löschen. Unternehmen und Organisationen müssen diese Rechte respektieren und entsprechende Maßnahmen ergreifen, um sie umzusetzen.

Verstöße gegen die DSGVO können zu hohen Geldstrafen führen. Unternehmen und Organisationen, die die Vorschriften nicht einhalten, können mit Geldbußen von bis zu 4 % des weltweiten Jahresumsatzes oder 20 Millionen Euro bestraft werden, je nachdem, welcher Betrag höher ist.

Insgesamt stellt die DSGVO sicher, dass Unternehmen und Organisationen verantwortungsbewusst und transparent mit personenbezogenen Daten umgehen und dass den betroffenen Personen mehr Kontrolle über ihre Daten gegeben wird.

Gesundheitstelematikgesetz

Das Gesundheitstelematikgesetz (eHealth-Gesetz) ist ein Gesetz in Deutschland, das die elektronische Vernetzung und den Austausch von Daten im Gesundheitswesen regelt. Es soll die Versorgung der Patienten verbessern und den Datenschutz gewährleisten.

Das Gesetz zielt darauf ab, die Kommunikation zwischen Ärzten, Krankenhäusern und anderen Gesundheitseinrichtungen zu verbessern, indem es eine elektronische Plattform schafft, auf der medizinische Daten sicher ausgetauscht werden können. Ziel ist es, die Qualität der Versorgung zu erhöhen, Fehler zu vermeiden und die Effizienz im Gesundheitswesen zu steigern.

Das Gesundheitstelematikgesetz umfasst verschiedene Maßnahmen, wie zum Beispiel:

Die Einführung einer elektronischen Patientenakte, in der medizinische Daten von verschiedenen Einrichtungen gespeichert werden können.

Die Einführung einer elektronischen Gesundheitskarte, die die Identität des Patienten und seine Versicherungsdaten enthält und bei der Abrechnung von medizinischen Leistungen verwendet wird.

Die Schaffung von sicheren Kommunikationsnetzwerken und -systemen, um den sicheren Austausch von medizinischen Daten zu gewährleisten.

Die Festlegung von Standards und Anforderungen an die Sicherheit von medizinischen Daten, um sicherzustellen, dass sie vor unbefugtem Zugriff und Missbrauch geschützt sind.

Das Gesundheitstelematikgesetz soll sicherstellen, dass der Austausch von medizinischen Daten im Gesundheitswesen sicher und effektiv erfolgt, während gleichzeitig der Schutz der personenbezogenen Daten gewährleistet wird.

Diese Gesetze sind wichtig, um sicherzustellen, dass unsere persönlichen Daten und unsere Gesundheitsdaten sicher aufbewahrt werden und vor Missbrauch geschützt sind.

Kommunikationsprotokolle

FTP

FTP (File Transfer Protocol) ist ein Protokoll zur Übertragung von Dateien zwischen Computern im Netzwerk oder über das Internet. Es ist ein relativ altes Protokoll und bietet keine Verschlüsselung, was es anfällig für Man-in-the-Middle-Angriffe und andere Sicherheitsrisiken macht.

SFTP

SFTP (Secure File Transfer Protocol) ist eine erweiterte Version des FTP-Protokolls und bietet eine sichere Möglichkeit zur Übertragung von Dateien zwischen Computern. Es verschlüsselt alle Datenübertragungen und bietet somit ein höheres Maß an Sicherheit als herkömmliches FTP.

HTTP

HTTP (Hypertext Transfer Protocol) ist ein Protokoll zur Übertragung von Webinhalten wie HTML-Seiten und anderen Ressourcen im Internet. Es ist das grundlegende Protokoll, das für die Kommunikation zwischen Webbrowsern und Webservern verwendet wird. Es bietet jedoch keine Verschlüsselung, was bedeutet, dass es anfällig für Man-in-the-Middle-Angriffe und andere Sicherheitsrisiken ist.

HTTPS

HTTPS (Hypertext Transfer Protocol Secure) ist eine sichere Version des HTTP-Protokolls. Es verschlüsselt alle Daten, die zwischen einem Client und einem Server ausgetauscht werden, und bietet somit ein höheres Maß an Sicherheit und Schutz vor Datenmanipulation und -diebstahl. Es wird oft für sicherheitskritische Transaktionen wie Online-Banking und E-Commerce-Transaktionen verwendet.

SMTP

Ein weiteres Protokoll, das für die Übertragung von E-Mails verwendet wird, ist das SMTP-Protokoll (Simple Mail Transfer Protocol). SMTP wird verwendet, um E-Mails von einem E-Mail-Client an einen E-Mail-Server und von einem E-Mail-Server an einen anderen E-Mail-Server zu übertragen. Es wird von vielen E-Mail-Diensten und E-Mail-Clients verwendet.

TCP

TCP ist ein Protokoll, das die Übertragung von Daten zwischen Geräten regelt, während IP die Adressierung und Übertragung von Datenpaketen im Netzwerk ermöglicht. Zusammen bilden sie ein System, das die Übertragung von Daten zwischen Geräten auf verschiedenen Netzwerken ermöglicht.

TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) ist eine Sammlung von Netzwerkprotokollen, die für die Übertragung von Daten zwischen Computern im Internet oder in anderen Netzwerken verwendet werden. Es handelt sich um ein Standard-Netzwerkprotokoll, das viele Anwendungen und Geräte unterstützen, einschließlich Webbrowsern, E-Mail-Clients, Netzwerkdruckern und Netzwerkspeichergeräten.
TCP/IP ist das grundlegende Protokoll, das für die Kommunikation im Internet und in vielen anderen Netzwerken verwendet wird. Es bietet eine zuverlässige und robuste Möglichkeit, Daten zwischen Geräten zu übertragen, und ist ein grundlegendes Konzept, das jeder Netzwerkadministrator und IT-Experte verstehen sollte.

UDP

UDP (User Datagram Protocol) ist ein Netzwerkprotokoll, das für die Übertragung von Daten zwischen Computern im Internet oder in anderen Netzwerken verwendet wird. Im Gegensatz zu TCP, einem anderen wichtigen Netzwerkprotokoll, das eine zuverlässige und robuste Datenübertragung gewährleistet, ist UDP eher auf eine schnelle und einfache Übertragung von Daten ohne Überprüfung der Zuverlässigkeit oder Wiederholung ausgelegt.

UDP wird häufig in Anwendungen wie Audio- oder Video-Streaming verwendet, wo Echtzeitübertragungen wichtiger sind als die Gewährleistung einer vollständigen und zuverlässigen Übertragung. Es wird auch für einige Online-Spiele und andere Anwendungen verwendet, bei denen schnelle Übertragung wichtiger ist als Zuverlässigkeit oder Fehlerkorrektur.

UDP ist ein wichtiges Konzept, das jeder Netzwerkadministrator und IT-Experte verstehen sollte, da es ein grundlegendes Protokoll ist, das für die Übertragung von Daten im Internet und in vielen anderen Netzwerken verwendet wird.

DNS

Ein weiteres wichtiges Netzwerkprotokoll ist das DNS-Protokoll (Domain Name System). DNS wird verwendet, um Domainnamen (wie example.com) in IP-Adressen umzuwandeln, die von Netzwerkgeräten verwendet werden können, um andere Geräte im Netzwerk zu finden. Ohne DNS müssten Benutzer die IP-Adressen von Websites und anderen Netzwerkressourcen manuell eingeben, was unpraktisch und fehleranfällig sein kann.

DDOS

DDoS (Distributed Denial of Service) ist ein Angriff auf ein Computersystem, bei dem ein Netzwerk von vielen Computern verwendet wird, um das System durch eine Überlastung mit Anfragen lahmzulegen. Der Zweck eines DDoS-Angriffs ist es, die Verfügbarkeit des Systems zu beeinträchtigen, indem der Server mit einer hohen Anzahl von Anfragen überflutet wird, so dass er nicht mehr reagiert oder nicht mehr erreichbar ist.

Die DDoS-Attacke erfolgt in der Regel über eine Vielzahl von infizierten Geräten, die als "Botnet" bezeichnet werden. Diese Geräte können mit Malware infiziert werden, die es Angreifern ermöglicht, sie fernzusteuern, um Anfragen an das Ziel-System zu senden. Der Angreifer nutzt dabei die Tatsache aus, dass die Geräte in einem Botnet oft schlecht geschützt sind und häufig über eine schnelle Internetverbindung verfügen.

DDoS-Angriffe können erhebliche Schäden verursachen, insbesondere wenn sie auf kritische Systeme wie Banken, Regierungsbehörden oder Krankenhäuser abzielen. Die Systeme können durch die Überlastung mit Anfragen unzugänglich gemacht werden, was zu Ausfallzeiten, Datenverlusten und sogar finanziellen Verlusten führen kann.

Um sich vor DDoS-Angriffen zu schützen, ist es wichtig, geeignete Sicherheitsmaßnahmen zu ergreifen, wie z.B. die Verwendung von Firewalls, die Begrenzung der Bandbreite für den Netzwerkverkehr und die Überwachung des Netzwerkverkehrs auf Anomalien. Es ist auch wichtig, dass Unternehmen und Organisationen regelmäßig Backups von wichtigen Daten erstellen, um im Falle eines Angriffs eine schnelle Wiederherstellung zu ermöglichen.

Einfache Definition

Eine DDoS-Attacke (Distributed Denial of Service) ist ein Angriff auf ein Computersystem, bei dem ein Netzwerk von vielen Computern verwendet wird, um das System durch eine Überlastung mit Anfragen lahmzulegen. Das Ziel eines DDoS-Angriffs ist es, die Verfügbarkeit

des Systems zu beeinträchtigen, indem der Server mit einer hohen Anzahl von Anfragen überflutet wird, so dass er nicht mehr reagiert oder nicht mehr erreichbar ist.

Was tun, wenn sowas passiert:

Im Falle einer DDoS-Attacke auf eine Gesundheitsorganisation gibt es mehrere Schritte, die unternommen werden sollten:

- Melden Sie den Angriff: Sobald eine DDoS-Attacke festgestellt wird, sollte das IT-Team der Organisation den Vorfall sofort melden. Sie können sich an spezialisierte Sicherheitsfirmen wenden, um Unterstützung bei der Bekämpfung des Angriffs zu erhalten.
- Bereiten Sie einen Notfallplan vor: Es ist wichtig, einen Notfallplan für DDoS-Attacken zu haben, der die erforderlichen Maßnahmen und Verfahren zur Eindämmung des Angriffs enthält. Die Mitarbeiter sollten über den Plan geschult und die notwendigen Ressourcen sollten zur Verfügung gestellt werden.
- Schützen Sie das Netzwerk: Es ist wichtig, das Netzwerk der Organisation zu schützen, indem geeignete Sicherheitsmaßnahmen ergriffen werden, wie z.B. die Verwendung von Firewalls, Intrusion-Detection-Systemen und anderen Sicherheitsvorkehrungen. Das Netzwerkverkehr sollte auch auf Anomalien überwacht werden, um mögliche Angriffe zu erkennen.
- Backup-Strategie: Eine regelmäßige Datensicherung sollte Teil des IT-Sicherheitskonzepts sein, um im Falle eines Angriffs die Daten wiederherstellen zu können. Die Backups sollten an einem sicheren Ort gespeichert werden.
- Kommunikation: Es ist wichtig, eine klare Kommunikationsstrategie zu haben, um die Kunden, Patienten und Mitarbeiter über den Angriff und die getroffenen Maßnahmen zu informieren. Eine transparente Kommunikation kann dazu beitragen, das Vertrauen der Öffentlichkeit wiederherzustellen und den Schaden zu begrenzen.
- Zusammenarbeit: Eine Zusammenarbeit mit anderen Organisationen und Sicherheitsfirmen kann bei der Bekämpfung des Angriffs helfen. Durch die Zusammenarbeit können Informationen und Ressourcen ausgetauscht werden, um den Angriff schnell zu bekämpfen.

DDoS-Attacken können schwerwiegende Auswirkungen auf Gesundheitsorganisationen haben und sollten daher ernst genommen werden. Eine schnelle Reaktion, eine angemessene Schulung der Mitarbeiter und die Umsetzung geeigneter Sicherheitsvorkehrungen können jedoch dazu beitragen, das Risiko von Angriffen zu minimieren und den Schaden zu begrenzen.

Malware

Malware (kurz für "malicious software") ist ein Oberbegriff für jede Art von schädlicher Software, die darauf abzielt, ein Computersystem oder ein Netzwerk zu infiltrieren und schädliche Aktivitäten auszuführen. Dazu gehören beispielsweise Viren, Trojaner, Würmer und Spyware.

Die Funktionsweise von Malware kann sehr unterschiedlich sein, aber im Allgemeinen infiziert sie ein System, indem sie eine Schwachstelle ausnutzt oder durch Social Engineering-Methoden wie Phishing oder Spear-Phishing Angriffe auf den Nutzer ausführt. Sobald die

Malware in ein System eingedrungen ist, kann sie verschiedene schädliche Aktivitäten ausführen, wie z.B. Daten stehlen, Daten verschlüsseln oder das System beschädigen. Malware kann verschiedene Ziele attackieren, wie beispielsweise:
Nutzerdaten wie Benutzernamen, Passwörter und Kreditkarteninformationen stehlen
Dateien auf dem System verschlüsseln oder löschen
Das System oder Netzwerk verlangsamen oder lahmlegen
Schädliche Software auf dem System installieren
Spam-E-Mails versenden oder andere Systeme angreifen
Um sich vor Malware-Angriffen zu schützen, sollten Nutzer sicherstellen, dass sie ihr System mit aktuellen Antivirus- und Anti-Malware-Software schützen, regelmäßige Sicherheitsupdates durchführen und verdächtige E-Mails und Links nicht öffnen. Es ist auch ratsam, die Nutzer über die Risiken und Gefahren von Malware-Angriffen zu schulen und sie über die aktuellen Bedrohungen und Sicherheitsmaßnahmen auf dem Laufenden zu halten.

Einfache Definition:

Malware (kurz für "malicious software") ist eine Art von schädlicher Software, die darauf abzielt, ein Computersystem oder ein Netzwerk zu infiltrieren und schädliche Aktivitäten auszuführen. Dazu gehören beispielsweise Viren, Trojaner, Würmer und Spyware.

Was ist zu tun:

Wenn eine Gesundheitsorganisation von einer Malware-Attacke betroffen ist, sollte sie umgehend Maßnahmen ergreifen, um den Angriff zu stoppen und die betroffenen Systeme zu sichern. Hier sind einige Schritte, die die Organisation durchführen kann:

- Beenden Sie die Verbindung: Wenn eine verdächtige Verbindung oder ein verdächtiger Datenverkehr erkannt wird, sollten alle betroffenen Geräte oder Systeme sofort von der Netzwerkverbindung getrennt werden.
- Überprüfen Sie die Systeme: Überprüfen Sie alle betroffenen Systeme und Geräte, um festzustellen, ob sie infiziert sind oder Malware enthalten. Wenn eine Infektion festgestellt wird, sollte das betroffene System isoliert und untersucht werden.
- Ändern Sie Passwörter: Ändern Sie alle betroffenen Passwörter und stellen Sie sicher, dass sie sicher und einzigartig sind. Überprüfen Sie auch alle Konten und stellen Sie sicher, dass sie nicht unbefugt genutzt werden.
- Informieren Sie die Behörden: Wenn es sich um einen schwerwiegenden Vorfall handelt, sollten die zuständigen Behörden informiert werden, um eine Untersuchung einzuleiten und gegebenenfalls den Angriff zu stoppen.
- Entfernen Sie die Malware: Entfernen Sie alle infizierten Dateien und Programme von betroffenen Systemen. Dazu sollten Sie spezielle Antivirus- und Anti-Malware-Software einsetzen, um die Malware zu entfernen.
- Verbessern Sie die Sicherheit: Stellen Sie sicher, dass alle Systeme und Geräte mit den neuesten Sicherheitsupdates und Patches aktualisiert sind und setzen Sie zusätzliche Sicherheitsmaßnahmen wie Firewalls und Intrusion Detection-Systeme ein, um zukünftige Angriffe zu verhindern.

Es ist wichtig, schnell zu handeln, um den Angriff zu stoppen und die Sicherheit des Systems wiederherzustellen, um weitere Schäden zu vermeiden.

Man-in-the-middle

Ein Man-in-the-Middle-Angriff (MITM-Angriff) ist eine Art von Cyberangriff, bei dem ein Angreifer die Verbindung zwischen zwei Kommunikationspartnern abfängt und manipuliert. Der Angreifer kann dann in der Lage sein, Informationen zu stehlen, zu manipulieren oder zu injizieren, ohne dass die betroffenen Parteien davon erfahren.

Der Angreifer nutzt dabei eine Schwachstelle in der Netzwerksicherheit, um die Verbindung abzufangen und sich zwischen die beiden Parteien zu setzen. Sobald der Angreifer zwischen den beiden Parteien steht, kann er den Datenverkehr abfangen, analysieren und manipulieren, indem er z.B. Nachrichten löscht oder ändert.

Ein typisches Szenario für einen MITM-Angriff ist eine öffentliche WLAN-Verbindung, die von vielen Menschen genutzt wird. Der Angreifer kann sich in diesem Fall als ein legitimer Access Point ausgeben und die Verbindung abfangen, um Daten zu stehlen oder zu manipulieren.

Ein weiteres Beispiel für einen MITM-Angriff ist eine Phishing-E-Mail, die den Empfänger dazu bringt, auf einen bösartigen Link zu klicken. Der Angreifer kann dann den Datenverkehr zwischen dem Opfer und der angegriffenen Webseite abfangen und die Eingaben des Opfers, wie z.B. Benutzernamen und Passwörter, stehlen.

Um sich vor MITM-Angriffen zu schützen, sollten die Nutzer sicherstellen, dass sie ihre Verbindungen über sichere Protokolle wie HTTPS und SSL/TLS verschlüsseln und auf verdächtige E-Mails und Links achten.

Einfache Definition:

Ein Man-in-the-Middle-Angriff (MITM-Angriff) ist ein Cyberangriff, bei dem ein Angreifer die Verbindung zwischen zwei Kommunikationspartnern abfängt und manipuliert, um Informationen zu stehlen oder zu manipulieren. Der Angreifer nutzt dabei eine Schwachstelle in der Netzwerksicherheit, um sich zwischen die beiden Parteien zu setzen und den Datenverkehr abzufangen, zu analysieren oder zu manipulieren.

Was ist zu tun bei sowas:

Wenn eine Gesundheitsorganisation von einem Man-in-the-Middle-Angriff betroffen ist, sollte sie umgehend Maßnahmen ergreifen, um den Angriff zu stoppen und die betroffenen Systeme zu sichern. Hier sind einige Schritte, die die Organisation durchführen kann:

- Beenden Sie die Verbindung: Wenn eine verdächtige Verbindung oder ein verdächtiger Datenverkehr erkannt wird, sollten alle betroffenen Geräte oder Systeme sofort von der Netzwerkverbindung getrennt werden.
- Überprüfen Sie die Systeme: Überprüfen Sie alle betroffenen Systeme und Geräte, um festzustellen, ob sie infiziert sind oder Malware enthalten. Wenn eine Infektion festgestellt wird, sollte das betroffene System isoliert und untersucht werden.
- Ändern Sie Passwörter: Ändern Sie alle betroffenen Passwörter und stellen Sie sicher, dass sie sicher und einzigartig sind. Überprüfen Sie auch alle Konten und stellen Sie sicher, dass sie nicht unbefugt genutzt werden.
- Informieren Sie die Behörden: Wenn es sich um einen schwerwiegenden Vorfall handelt, sollten die zuständigen Behörden informiert werden, um eine Untersuchung einzuleiten und gegebenenfalls den Angriff zu stoppen.
- Verbessern Sie die Sicherheit: Stellen Sie sicher, dass alle Systeme und Geräte mit den neuesten Sicherheitsupdates und Patches aktualisiert sind und setzen Sie zusätzliche Sicherheitsmaßnahmen wie Firewalls und Intrusion Detection-Systeme ein, um zukünftige Angriffe zu verhindern.

Es ist wichtig, schnell zu handeln, um den Angriff zu stoppen und die Sicherheit des Systems wiederherzustellen, um weitere Schäden zu vermeiden.

Phishing

Was ist PHISHING und worauf muss ich achten?

Phishing ist eine Cyberangriffsform, bei der der Angreifer Nachrichten an eine Person, ein Unternehmen oder einer ganzen Organisation verschickt, mit dem Ziel, sensible Informationen oder Daten vom Empfänger zu entlocken oder den Empfänger zum Download von einem Schadcode zu verführen, um so den jeweiligen Arbeitgeber zu schaden. Die Informationen, welche der Angreifer versucht zu entlocken sind personenbezogene Daten, Passwörter, Login- Daten oder Transaktionsnummern. Beim Phishing erschleichen sich die Betrüger das Vertrauen der Empfänger, in dem sie irreführende Behauptungen aufstellen oder ein Szenario inszenieren, welches eine bestimmte Reaktion provozieren soll. Meistens geben sich diese Betrüger als vertrauenswürdige Instanz aus, wie z.B. eine Bank, um so die Opfer zu ködern und diese zu der gewünschten Handlung zu bewegen.
Die beliebteste Form des Phishings sind Phishing- E- Mails. Dabei handelt es sich um gefälschte E- Mails, mit denen versucht wichtige Daten vom Empfänger zu stehlen. Dabei verwenden Angreifer eine E- Mail- Adresse, welche dem Anschein nach von einem vertrauenswürdigen Absender stammen könnte. In der E- Mail wird meistens aufgefordert auf einen Link zu klicken oder seine Angaben zu bestätigen oder zu aktualisieren. Wird dem nachgegangen wird der Empfänger auf eine gefälschte Website weitergeleitet, welche dann die sensiblen Daten abgreift.

Welche Punkte für welche Berufsgruppe zu beachten sind
Personal der Gesundheitsberufe
Die Angriffsform des Phishings ist vor allem im Gesundheitsbereich anzutreffen. Vor allem die Zeit der COVID- 19 Pandemie wurden von Angreifern ausgenutzt, um sensible Daten abzufangen. Hier sind zwei Beispiele, die ich zum Thema gefunden habe
Vor allem im Gesundheitsbereich bringen Cyberangriffe ein hohes Risiko mit sich, da sich um sensible personenbezogene Daten handelt, welche Angreifer versuchen zu entlocken, und daher könnte auch die Sicherheit und/oder Gesundheit eines Patienten involviert sein. Aus diesem Grund ist es sehr wichtig, dass das Personal Phishing- E- Mails oder Websites erkennen können. Diese Punkte muss das Personal im Gesundheitsbereich beachten, um Phishing zu erkennen:

- Überprüfung der Absender- Adresse: Da häufig sich Angreifer als vertrauensvolle Instanzen oder Unternehmen ausgeben, sehen die E- Mail- Adressen zu dem Original sehr ähnlich, aber dennoch gibt es kleine Unterschiede. Aus diesem Grund sollte man unbedingt die Absender- Adresse überprüfen.

- Überprüfung des Betreffs: Sollte der Betreff merkwürdig rüberkommen, dann ist Vorsicht geboten und es sollte einem bewusst sein, dass es sich möglicherweise, um eine Phishing- E- Mail handelt.

- Überprüfung der Anrede: Es ist üblich, dass in Phishing- E- Mails die Empfänger nicht persönlich angesprochen werden. Vor allem wenn eine E- Mail von einem Unternehmen stammen soll und die Anrede „ Sehr geehrte Damen

und Herren“ ist, kann dies ein Anzeichen für Phishing sein. Jedoch muss in dem Fall auch nach weiteren Anzeichen Ausschau gehalten werden.

- Überprüfung der Formatierung: Phishing- Mails weisen oft eine schlechte Rechtschreibung oder Syntax auf. Auch Reste von HTML- Behlen wie   oder <p> deuten auf Phishing. Zudem ist auch ein uneinheitliches Layout oder ein Wechsel der Schriftart ein Zeichen.

- Überprüfung, ob man zur Angabe von persönlichen Daten ausgefordert wird: Phishing- Mails sind dafür bekannt, dass die Empfänger aufgefordert werden persönliche Daten zu bestätigen. Einige dieser E- Mails enthalten auch Bedrohungen wie „Wenn Sie Ihre Daten nicht bestätigen, wird Ihr Konto gesperrt“. Dies geschieht auch in Kombination mit Fristsetzungen. Die Forderungen können vertrauliche Daten, wie PIN, TAN, Passwort, Adresse oder auch ein Geburtsdatum sein. Es ist wichtig sich im Bewusstsein zu rufen, dass echte Unternehmen nicht nach solchen Daten in einer E-Mail fragen.

- Überprüfung von Links auf Websites: Phishing- Mails könne auch mit Links auch auf Websites verweisen. Diese Links sehen dem Original sehr ähnlich. Daher sollte man, überprüfen, ob diese Links merkwürdige Zahlen- und Buchstaben-Kombinationen enthalten. Wird auf die Website geklickt, so könnte ein Virus unbewusst heruntergeladen werden.

- Überprüfung der Anhänge: Häufig enthalten Phishing- Mails Anhänge, welche meistens keine ordentlichen Namen haben, sondern nur Zeichenfolge. Aussehen können sie wie ein Bild oder PDF- Datei. Beim Herunterladen wird man entweder auf eine gefälschte Website weitergeleitet oder es wird ein Computervirus gedownloadet. Der Anhang einer Phishing- Mail darf nicht geöffnet oder heruntergeladen werden!

- Phishing- Mails betroffenen Unternehmen melden: Gibt es die Vermutung, dass eine gefälschte E- Mail von einem bekannten Unternehmen erhalten worden ist, sollte dieses Unternehmen über dessen in Kenntnis gesetzt werden. So kann einerseits sichergestellt werden, ob die E- Mail tatsächlich vom Unternehmen stammt und andererseits weiß das Unternehmen, dass in seinem Namen gefälschte E- Mails verschickt werden.

- In der Gesundheitsorganisation bekanntmachen: Damit nicht andere Mitarbeiter auf dem Phishing- Angriff reinfallen, muss der Vorfall in der Organisation schnellstmöglich bekannt gemacht werden. Am besten ist es eine E-Mail mit einem Screenshot von der Phishing- Mail an die gesamte Organisation zu verschicken. Man kann den Vorfall auch zuerst beim Vorgesetzten bekanntgeben und dieser kümmert sich dann um die Bekanntgabe.

Die oben genannten Punkte sind auch vom Personal der Verwaltung, der Haus- und Betriebstechnik sowie vom Personal der Medizintechnik zu beachten.

Smishing

Was ist SMISCHING und worauf muss ich achten!

Genau wie Phishing handelt sich auch beim Smishing um eine Cyberangriffsform. Smishing setzt sich aus den Worten „SMS“ und „Phishing“ zusammen. Bei dieser Cyberangriffsattacke werden gefälschte Textnachrichten verschickt mit dem gleichen Ziel wie beim Phishing- die Angreifer möchten sensible persönliche Daten entlocken. Smishing- Attacken sind stark im Kommen, da viel mehr Leute skeptisch gegenüber E- Mails sind als SMS. Von Phishing haben die meisten gehört und selber schon Erfahrung damit gehabt und aus diesem Grund sind viele vorsichtig gegenüber verdächtigen E- Mails, jedoch schienen die meisten Menschen unvorsichtiger gegenüber SMS zu sein.
Smishing- SMS enthalten einen für den Empfänger schädlichen Inhalt. In erster Linie versuchen Angreifen mit dieser Form der Cyberattacke Bankverbindungen, Passwörter oder andere sensible Daten vom Opfer zu entlocken. Um dies zu erreichen wird manchmal sogar eine schädliche Software auf dem Gerät des Opfers installiert. Social Engineering* wird häufig in Kombination mit Smishing eingesetzt. Angreifer sind zudem in der Lage persönliche Informationen, wie z.B. Name und Adresse, welche sie aus öffentlichen Online- Tools bekommen haben, einzusetzen. So kann der Smisher den Namen und Standort des Empfängers verwenden, um diesen direkt anzusprechen. Durch diese Details ist die Nachricht aussagekräftiger. In der SMS ist dann ein Link enthalten, welcher auf Phishing-Seiten für Anmeldeinformationen weiterleitet oder zu einer Malware (=Überbegriff für verschiede Arten von schädlichen Programmen) führt.
*Social Engineering: Social Engineering befasst sich mit Manipulation und wird häufig von Cyberkriminelle benützt. Angreifer verwenden dabei Informationen aus sozialen Netzwerken und versuchen die menschliche Natur für ihre Zwecke auszunutzen. Dabei setzten die Angreife auf Gefühle wie Angst, Gier, Empathie und versuchen so den Denkprozessen der Empfänger zu manipulieren.

Welche Punkte für welche Berufsgruppe zu beachten sind

- Überprüfung des Absenders: Genau wie beim Phishing versuchen Angreifer das Vertrauen der Opfer zu gewinnen indem sie die Identität von vertrauenswürdigen Instanzen, Unternehmen oder Organisationen annehmen. Erscheint eine SMS als merkwürdig, sollte man bei der entsprechenden Organisation oder Unternehmen nachfragen. Zudem sollte bewusst sein, dass vertrauenswürdige Instanzen, Organisationen oder Unternehmen niemals eine SMS senden würde, in der man aufgefordert wird, seine Daten anzugeben. Aus diesem Grund sollte man zweimal den Namen des Absenders überprüfen.

- Überprüfung des Inhalts: Beinhaltet die SMS beispielsweise die Bekanntgabe über ein Wettbewerb an dem Sie angeblich gewonnen haben, dann handelt es sich höchstwahrscheinlich um eine Smishing- Attacke. Das selbe Konzept kann auch mit einer Bestellungsinformation erscheinen. Wichtig hierbei ist nicht auf den Link zu klicken, die Organisation in der Sie arbeiten schnellstmöglich zu informieren und anschließend die Nachricht zu löschen. Es könnte hilfreich sein davor ein Screenshot zu machen und diesen bei der Bekanntgabe der Organisation mit bsw. einer E- Mail im Anhang mitzuverschicken. Der Screenshot kann auch eine Absicherung sein, falls eine weitere Smishing- Attacke folgt. In

dem Fall kann man die SMS mit dem Screenshot vergleichen und so nach Muster Ausschau halte.

Ein weiterer Punkt auf dem man achten muss ist, ob man aufgefordert wird, eine App herunterzuladen. Denn dabei könnte es sich um eine Malware handeln.

- Überprüfung, ob nach persönlichen Informationen gefragt wird: Angreifer können sich sogar als Personen aus dem direkten Umfeld ausgeben um an Informationen zu kommen. Falls Sie aufgefordert werden von jemanden, welcher sich als eine Person aus Ihrem Umfeld auszugeben versucht, Informationen anzugeben, dann ist es klüger erstmals die Identität des Absenders zu überprüfen, indem Kontakt zu der entsprechenden Person aus Ihrem Umfeld aufgenommen wird.

Die oben genannten Punkte sind von allen Berufsgruppen (Personal des Gesundheitswesens, Personal der Verwaltung, Personal Haus- und Betriebstechnik und Personal der Medizintechnik) zu beachten.

Die beste Möglichkeit sich als Unternehmen oder Organisation vor Phishing- und Smishing-Attacken zu schützen ist, die Angestellten zum Thema Cybersicherheit schulen zu lassen. So können sie über die Merkmale aufgeklärt werden und ihnen kann auch bewusst gemacht werden, welche Risiken solche Attacken darstellen.

Ransomware

Eine Ransomware-Attacke ist ein Cyberangriff, bei dem ein Angreifer schädliche Software auf das System eines Opfers einschleust, um dessen Daten und Systeme zu verschlüsseln und unzugänglich zu machen. Der Angreifer fordert dann ein Lösegeld vom Opfer, um die Daten wiederherzustellen und den Zugriff auf das System wiederherzustellen.
Die Ransomware kann auf verschiedene Arten in das System des Opfers eindringen, wie z.B. durch E-Mail-Anhänge, infizierte Websites, Social Engineering oder Schwachstellen in Software und Systemen. Sobald die Ransomware in das System eindringt, beginnt sie, die Daten des Opfers zu verschlüsseln, so dass der Opfer keinen Zugriff mehr darauf hat.
Die Ransomware verwendet in der Regel einen starken Verschlüsselungsalgorithmus, der es nahezu unmöglich macht, die verschlüsselten Daten, ohne den richtigen Entschlüsselungsschlüssel wiederherzustellen. Der Angreifer fordert dann ein Lösegeld, um den Entschlüsselungsschlüssel zu erhalten und den Zugriff auf die Daten wiederherzustellen.
Die Opfer haben oft nur wenige Optionen, wenn sie von einer Ransomware-Attacke betroffen sind. Sie können das Lösegeld zahlen, um den Zugriff auf ihre Daten wiederherzustellen, oder sie können versuchen, ihre Daten aus Backups wiederherzustellen oder die Hilfe von Experten in Anspruch nehmen.
Ransomware-Attacken können schwerwiegende Auswirkungen haben, insbesondere im Gesundheitswesen, da hier sehr sensible Patientendaten betroffen sein können. Es ist daher wichtig, regelmäßige Backups zu erstellen, Sicherheitslücken in Software und Systemen zu minimieren und Mitarbeiter über die Risiken und Folgen von Ransomware-Attacken zu schulen, um das Risiko von Angriffen zu minimieren.

Einfache und simple Definition:

Eine Ransomware-Attacke ist ein Angriff auf ein Computersystem, bei dem Schadsoftware verwendet wird, um Daten des Opfers zu verschlüsseln und unzugänglich zu machen. Der Angreifer fordert dann ein Lösegeld, um den Zugriff auf die Daten wiederherzustellen.

Was machen, wenn sowas passiert:

Im Falle einer Ransomware-Attacke auf eine Gesundheitsorganisation sollte dieser folgende Schritt unternehmen:

- Sofortige Trennung des betroffenen Netzwerks vom Internet und von anderen Netzwerken, um eine Ausbreitung der Ransomware auf andere Systeme zu verhindern.
- Benachrichtigung der IT-Abteilung und des IT-Sicherheitsbeauftragten, um die Situation schnell zu analysieren und geeignete Maßnahmen zur Eindämmung der Infektion zu ergreifen.
- Sicherung von wichtigen Daten und Systemen, um Datenverluste zu minimieren.
- Einrichtung eines Notfallteams, das sich mit der Ransomware-Attacke befasst und Maßnahmen zur Wiederherstellung der Systeme und Daten koordiniert.
- Erstellung von Backups von kritischen Daten und Systemen, um eine schnelle Wiederherstellung der Systeme zu ermöglichen.
- Analyse der Ransomware und der Art des Angriffs, um geeignete Gegenmaßnahmen zu ergreifen.
- Entfernung der Ransomware von den betroffenen Systemen und Netzwerken.
- Meldung des Vorfalls an die zuständige Aufsichtsbehörde und an die betroffenen Patienten, sofern personenbezogene Daten betroffen sind.
- Implementierung von Maßnahmen, um zukünftige Ransomware-Attacken zu verhindern, wie z.B. regelmäßige Backups, Aktualisierung von Systemen und Software, Schulung von Mitarbeitern im Umgang mit Ransomware-Attacken, etc.

Eine schnelle Reaktion auf eine Ransomware-Attacke ist entscheidend, um den Schaden zu minimieren und eine schnelle Wiederherstellung der betroffenen Systeme und Daten zu ermöglichen.

Was tun, wenn man kein Backup hat, oder keine Möglichkeit hat es zu umgehen?

Wenn es kein Backup gibt, dann wird es schwieriger, die Daten wiederherzustellen, nachdem eine Ransomware-Attacke stattgefunden hat. Hier sind einige Optionen, die in Betracht gezogen werden können:

- Zahlung des Lösegeldes: Die Angreifer fordern normalerweise ein Lösegeld, um die verschlüsselten Daten wieder freizugeben. Es gibt jedoch keine Garantie dafür, dass die Angreifer tatsächlich die Daten wiederherstellen, nachdem das Lösegeld gezahlt wurde. Darüber hinaus kann das Zahlen des Lösegeldes als Anreiz für die Angreifer dienen, weitere Ransomware-Attacken durchzuführen.
- Verwendung von Entschlüsselungs-Tools: Es gibt einige Entschlüsselungs-Tools, die kostenlos oder gegen eine Gebühr verfügbar sind. Diese Tools können jedoch nicht für alle Arten von Ransomware und Verschlüsselungsalgorithmen geeignet sein und möglicherweise nicht in der Lage sein, alle Daten wiederherzustellen.

- Wiederherstellung von Daten aus Schattenkopien: Einige Betriebssysteme erstellen automatisch Schattenkopien von Dateien, die als Teil der Systemwiederherstellung gespeichert werden. Diese Schattenkopien können verwendet werden, um ältere Versionen der Dateien wiederherzustellen, bevor sie durch die Ransomware verschlüsselt wurden.
- Expertenhilfe: Es kann sinnvoll sein, sich an einen IT-Sicherheitsexperten oder ein spezialisiertes Unternehmen zu wenden, um bei der Wiederherstellung der Daten zu helfen. Solche Experten können in der Lage sein, die Ransomware zu identifizieren und Maßnahmen zu ergreifen, um die verschlüsselten Daten wiederherzustellen.

Es ist wichtig zu beachten, dass es keine Garantie gibt, dass die Daten wiederhergestellt werden können, nachdem eine Ransomware-Attacke stattgefunden hat, insbesondere wenn kein Backup verfügbar ist. Es ist daher ratsam, regelmäßig Backups zu erstellen und andere Präventivmaßnahmen zu ergreifen, um die Auswirkungen von Ransomware-Attacken zu minimieren.

Weiteres zu beachten:

- Keine Zahlung des Lösegelds: Es wird empfohlen, das Lösegeld nicht zu zahlen, da dies die Angreifer ermutigen kann, weitere Angriffe durchzuführen. Darüber hinaus gibt es keine Garantie dafür, dass die Angreifer tatsächlich die Daten wiederherstellen, nachdem das Lösegeld gezahlt wurde.
- Schnelle Reaktion: Eine schnelle Reaktion auf einen Ransomware-Angriff ist entscheidend, um den Schaden zu minimieren und eine schnelle Wiederherstellung der betroffenen Systeme und Daten zu ermöglichen. Daher sollten Unternehmen und Organisationen einen Notfallplan für Ransomware-Attacken haben und sicherstellen, dass Mitarbeiter entsprechend geschult sind.
- Sicherheitsvorkehrungen: Es ist wichtig, Sicherheitsvorkehrungen zu treffen, um das Risiko von Ransomware-Attacken zu minimieren. Dazu gehört die Verwendung von Anti-Viren-Software und Firewalls, regelmäßige Updates von Betriebssystemen und Anwendungen, die Einschränkung von Berechtigungen für Mitarbeiter und die Schulung von Mitarbeitern im Umgang mit verdächtigen E-Mails und Anhängen.
- Backups: Es ist ratsam, regelmäßige Backups von wichtigen Daten zu erstellen und sicherzustellen, dass diese Backups an einem sicheren Ort gespeichert werden. Wenn eine Ransomware-Attacke stattfindet, können Backups verwendet werden, um die Daten schnell wiederherzustellen und die Auswirkungen des Angriffs zu minimieren.

Es ist wichtig zu beachten, dass Ransomware-Attacken sehr ernst sind und eine erhebliche Bedrohung für Unternehmen und Organisationen darstellen. Eine schnelle Reaktion, eine angemessene Schulung der Mitarbeiter und die Umsetzung geeigneter Sicherheitsvorkehrungen können jedoch dazu beitragen, das Risiko von Angriffen zu minimieren und den Schaden zu begrenzen.

SQL-Injection

SQL Injection ist eine Art von Cyberangriff, bei dem ein Angreifer bösartigen SQL-Code in eine Anwendung einschleust, um Zugriff auf vertrauliche Daten oder Systeme zu erlangen oder Schaden zu verursachen.
Der Angreifer nutzt dabei Schwachstellen in der Anwendung aus, um schädlichen SQL-Code einzuschleusen. Diese Schwachstellen können z.B. fehlende Validierung von Benutzereingaben oder unsichere Datenbankabfragen sein.
Durch die SQL Injection kann der Angreifer die Datenbank manipulieren und Abfragen ausführen, die er normalerweise nicht ausführen könnte. Beispielsweise kann ein Angreifer durch eine SQL Injection Zugriff auf Benutzerdaten erlangen, indem er eine Abfrage erstellt, die alle Benutzernamen und Passwörter in der Datenbank ausliest.
Ein weiteres Beispiel wäre die Änderung oder Löschung von Daten in der Datenbank. Hier könnte der Angreifer schädliche Abfragen erstellen, die es ihm ermöglichen, bestimmte Datensätze zu löschen oder zu manipulieren.
Um sich gegen SQL Injection-Angriffe zu schützen, sollten Entwickler sicherstellen, dass Benutzereingaben validiert werden und dass dynamisch generierte SQL-Abfragen sicher vorbereitet und ausgeführt werden. Es ist auch wichtig, dass alle Systeme und Anwendungen regelmäßig auf Schwachstellen überprüft und aktualisiert werden, um Angriffen vorzubeugen.

Einfache Definition:

SQL Injection ist eine Art von Cyberangriff, bei dem ein Angreifer schädlichen SQL-Code in eine Anwendung einschleust, um Zugriff auf vertrauliche Daten oder Systeme zu erlangen oder Schaden zu verursachen.

Was ist zu tun bei sowas:

Wenn eine Gesundheitsorganisation von einer SQL-Injection-Attacke betroffen ist, sollten sie umgehend Maßnahmen ergreifen, um den Angriff zu stoppen und die betroffenen Systeme zu sichern. Hier sind einige Schritte, die die Organisation durchführen kann:

- Beenden Sie die Verbindung: Trennen Sie alle betroffenen Geräte oder Systeme von der Netzwerkverbindung, um weitere Schäden zu vermeiden.
- Überprüfen Sie die Systeme: Überprüfen Sie alle betroffenen Systeme und Geräte, um festzustellen, ob sie infiziert sind oder SQL-Injection-Angriffe ausgesetzt sind. Wenn eine Infektion festgestellt wird, sollte das betroffene System isoliert und untersucht werden.
- Ändern Sie Passwörter: Ändern Sie alle betroffenen Passwörter und stellen Sie sicher, dass sie sicher und einzigartig sind. Überprüfen Sie auch alle Konten und stellen Sie sicher, dass sie nicht unbefugt genutzt werden.
- Entfernen Sie den schädlichen SQL-Code: Entfernen Sie den schädlichen SQL-Code aus der Anwendung, indem Sie die Schwachstellen identifizieren und schließen, die den Angriff ermöglicht haben.
- Verbessern Sie die Sicherheit: Stellen Sie sicher, dass alle Systeme und Geräte mit den neuesten Sicherheitsupdates und Patches aktualisiert sind und setzen Sie zusätzliche Sicherheitsmaßnahmen wie Firewalls und Intrusion Detection-Systeme ein, um zukünftige Angriffe zu verhindern.

Es ist wichtig, schnell zu handeln, um den Angriff zu stoppen und die Sicherheit des Systems wiederherzustellen, um weitere Schäden zu vermeiden.

Begrifflichkeiten

SOC

SOC steht für Security Operations Center und bezeichnet ein zentrales Überwachungs- und Analysezentrum, das für die Überwachung und Analyse der IT-Sicherheit in einem Unternehmen oder einer Organisation verantwortlich ist. Ein SOC sammelt Daten und Informationen aus verschiedenen Quellen wie Netzwerkgeräten, Servern, Endgeräten und Anwendungen und analysiert sie, um potenzielle Sicherheitsbedrohungen und Angriffe zu identifizieren und darauf zu reagieren. SOC-Teams bestehen aus IT-Sicherheitsexperten, die eng zusammenarbeiten, um Sicherheitsvorfälle zu untersuchen, zu bewerten und zu beheben. Durch die Implementierung eines SOC können Organisationen ihre IT-Sicherheit verbessern und schneller auf Bedrohungen und Angriffe reagieren.

CISO

CISO steht für Chief Information Security Officer und bezeichnet den Leiter der IT-Sicherheitsabteilung eines Unternehmens oder einer Organisation. Der CISO ist für die Planung, Umsetzung und Überwachung der IT-Sicherheitsstrategie und -programme verantwortlich und arbeitet eng mit anderen Führungskräften und IT-Teams zusammen, um sicherzustellen, dass die Sicherheitsziele des Unternehmens erreicht werden. Der CISO ist auch für die Identifizierung, Bewertung und Überwachung von Sicherheitsrisiken und Bedrohungen sowie für die Entwicklung von Plänen zur Risikobewältigung und -vermeidung zuständig. Der CISO muss über fundierte Kenntnisse in IT-Sicherheitspraktiken und -technologien verfügen sowie ein Verständnis für die Geschäftsziele und -prozesse des Unternehmens haben.

KOFÜ

KOFÜ steht für Koordinationsstelle für IT-Sicherheit im Gesundheitswesen und ist eine Einrichtung, die im Auftrag des Bundesministeriums für Gesundheit in Deutschland tätig ist. Die KOFÜ ist verantwortlich für die Koordination und Unterstützung von IT-Sicherheitsmaßnahmen im Gesundheitswesen und berät Gesundheitseinrichtungen bei der Umsetzung von IT-Sicherheitsrichtlinien und -standards. Die KOFÜ bietet auch Schulungen und Workshops für Mitarbeiter im Gesundheitswesen an, um das Bewusstsein für IT-Sicherheit zu erhöhen und sicherzustellen, dass die IT-Systeme im Gesundheitswesen sicher und geschützt sind.