ZAC-Nds. - Präventionsmaßnahmen und Angriffsszenarien

Stand der Präventionshinweise: 06.01.2022 07:41 Uhr

Stand der Angriffsszenarien: 06.01.2022 07:38 Uhr

Checklisten zu Präventionsmaßnahmen

Möchten Sie das Thema Cybersicherheit in Ihrem Unternehmen ernst nehmen? Hangeln Sie sich anhand dieser Checkliste durch die verschiedenen Themengebiete und prüfen Sie ob und wie Ihr Unternehmen aufgestellt ist.

Die Hinweise sind jeweils nicht abschließend, sondern decken nur die wichtigsten Bereiche der präventiven IT-Sicherheit ab.

Besprechen Sie die Hinweise und Fragen mit Ihrem IT-Dienstleister- bei entsprechender Kompetenz wird er auskunftsfähig sein und Ihre Fragen beantworten.

1. Schulung der MitarbeiterInnen

MitarbeiterInnen sollten über die Gefahren im Zusammenhang mit IT und der täglichen Arbeit aufgeklärt werden. Sie brauchen für Fragen im Zusammenhang mit IT eine feste, vertrauensvolle Ansprechperson. Zusätzlich sollte ein Sensibiliserung erfolgen, dass ungewöhnliche Vorfälle zeitnah an eine verantwortliche Person berichtet werden.

MitarbeiterInnen müssen darüber hinaus klare Regeln und Hinweise zur IT-Nutzung bekommen, dazu gehören z.B.

- Die zugelassene Art und Weise der Verwendung von privaten Komponenten (beispielsweise USB-Sticks) muss dargestellt werden
- Die private Internetnutzung ist zu regeln und ggf. technisch zu reglementieren
- Die Nutzung von privaten mobilen Endgeräten im Firmen-WLAN ist klar zu regeln bzw. zu unterbinden
- Die Wichtigkeit eines guten Passwortes muss dargestellt werden
- Die zugelassenen Datei-Endungen in der Unternehmenskommunikation sind festzulegen
- MitarbeiterInnen müssen die Gefahren kennen, die beispielsweise durch Makros in Office-Dokumenten entstehen können
- Es muss klar sein, dass ein installierter Virenscanner keinen absoluten Schutz vor Viren und Trojanern bietet
- Die Abläufe und Verantwortlichen in der Firma in Sachen Administration und Wartung von IT-Komponenten müssen benannt werden
- Die AnsprechpartnerInnen für technische Fragen oder ungewöhnliche Vorfälle muss bekannt, ansprechbar und hilfsbereit sein
- Die MitarbeiterInnen sind auf Verschwiegenheitspflichten, die Einhaltung der firmeneigenen Sicherheitsrichtlinien und möglichen Effekten bei Nicht-Beachtung hinzuweisen
- IT-gestützte Prozesse (bspw. die Art und Weise der Durchführung von Überweisungen)

sind mit Nennung der Gefahren zu beschreiben
- Eine Schulung hinsichtlich der Gefahren der unverschlüsselten und unsignierten Kommunikation via E-Mail ist notwendig, um die MA in die Lage zuversetzen, gefälschte E-Mailabsender oder manipulierte Ziel-Webseiten zu erkennen
- Nutzen Sie ggf. Online-Seminare, die verpflichtend für alle MitarbeiterInnen angeboten werden, um den sicheren Umgang mit z.B. E-Mails zu vermitteln
- Eine regelmäßige Auffrischung, z. B. jährlich mittels Online-Seminar und/oder kurzen Fragebogen, hilft bei einem stetigen Aufbau des Verständnisses der MitarbeiterInnen für die Gefahren

2. Notfallpläne

Es empfiehlt sich zu einzelnen Szenarien eine Notfallvorsorge zu treffen. Dazu kann man einzelne Varianten von Angriffen „durchspielen“.

Beispiel 1:
Was wäre wenn alle Daten des Unternehmens durch eine Ransomware (Verschlüsselungstrojaner) verschlüsselt sind?

- Kann der Betrieb weitergehen?
- Was funktioniert nicht mehr?
- Haben wir ein funktionierendes Backup?
- Wie lange dauert die Wiederherstellung der Daten?

Beispiel 2:
Was wäre wenn die Internetpräsenz des Unternehmens durch einen (DDOS)-Angriff für mehrere Stunden nicht mehr erreichbar ist?

- Entstehen dadurch Verluste?
- Müssen Vorkehrungen (DDOS-Schutz) im Vorfeld getroffen werden?
- Können eventuell Kundendaten von der Webpräsenz abfließen?
- Wer ist Ansprechpartner beim Provider?

Beispiel 3:
Ein mobiles Endgerät des Unternehmens wird entwendet.

- Welche Daten und Zugänge stehen dem Dieb zur Verfügung?
- Welche Maßnahmen müssen danach getroffen werden (Sperrung von Accounts, Neu-Vergabe von Passwörtern)
- Wird im Vorfeld eine Verschlüsselung auf den Endgeräten verwendet?

Sonstiges:

Klären Sie im Vorfeld die Ansprechpartner und Kontaktdaten von IT-Dienstleistern und der Polizei.

Teilen Sie Ihren Mitarbeitern mit, wen sie im Falle eines ungewöhnlichen Vorfalls zu kontaktieren haben.

Haben Sie eine alternative Kommunikationsmöglichkeit mit Ihren Mitarbeitern falls das E-Mailsystem nicht zur Verfügung steht? Wie erreichen Sie Ihre Mitarbeiter und teilen Ihnen beispielsweise mit, dass eine bestimmte E-Mail eine Schadsoftware enthält und nicht zu öffnen ist?

Haben Sie Ihre Notfalldokumente und Dokumentationen Offline? Zum Beispiel in einem Tresor? Bedenken Sie, dass Sie z.B. bei Ausfällen von Systemen ggf. auf Daten nicht mehr zugreifen können und alle notwendigen Informationen für die Notfallbearbeitung schnell anderweitig zugreifbar sein müssen.

3. Protokollierung

Um in einem Fall des Angriffs eine Lokalisierung des Problems und eine schnelle Behebung durchführen zu können, empfiehlt sich das Führen von Protokolldateien bzw. Logfiles. Dabei muss im Vorfeld eine Abwägung zwischen der Menge an Logdateien und dem späteren Nutzen getroffen werden. Auch rechtliche Aspekte bzgl. Aufbewahrungsfristen und Datensparsamkeit sind hier zu berücksichtigen. Eine Anonymisierung, Pseudonymisierung oder Aggregation kann notwendig sein.

Beispiel:
Welche Benutzeraktionen sollen protokolliert werden? Wenig Sinn ergibt die Protokollierung auf Ebene von Dateioperationen (Anlegen, Löschen etc.)- eher sinnvoll ist die Protokollierung von administrativen Aktionen (Anlegen, Löschen von Benutzern) oder auch der eigentliche Anmeldevorgang an einem Client.

Jedes eingesetzte System hat seine eigenen Log-Modalitäten und Besonderheiten:

- Eine FritzBox protokolliert nur solange wie sie in Betrieb ist - nach einem Neustart sind die Protokolldaten verloren
- Ein Mailserver protokolliert auf technischer Ebene die eingehenden und ausgehenden Mails (ohne Inhalt)
- Ein Webserver protokolliert auf IP-Ebene die eingehenden Verbindungen und die ausgelieferten Webseiten
- Eine Firewall protokolliert u.U. die abgewiesenen Verbindungen

Sonstiges:

Es besteht die Möglichkeit, Protokolldaten an einem zentralen Ort zusammenfließen zu lassen.

Das ergibt in einem nächsten Schritt die Möglichkeit, dass auf Basis der Protokollierung

auch ein Warnsystem implementiert werden kann, so dass z.B. die fehlgeschlagenen Anmeldeversuche an einem Client oder dem Mailsystem an einen Administrator gemeldet werden.

Integrierbar in ein zentrales Warnsystem wäre auch die Prüfung auf eine mögliche Kompromittierung der Firmenwebseite.

Wichtig bei der Protokollierung sind die Zeitsynchronisation zwischen den Systemen und die passende Einstellung bei den Zeitzonen. Am Besten es wird unternehmsweit in UTC protokolliert. Ohne dies wird eine Analyse über mehrere Systeme deutlich erschwert.

4. Dokumentation

Unabhängig von der Komplexität der IT-Infrastruktur empfiehlt sich eine Dokumentation der Gegebenheiten. Dazu gehört ein Netzplan (mit den eingesetzten Komponenten) und die deutliche Markierung jeglicher Einwahlmöglichkeiten bzw. Netzkopplungen.

Fragen, die in diesem Zusammenhang zu stellen sind:

- Wie ist der Zugang zum eigenen Netzwerk möglich?
- Gibt es einen WLAN-Accesspoint oder auch Remote-Administrationsmöglichkeiten (z.B. via RDP, Teamviewer etc.)?
- Welche Software-Versionen werden eingesetzt? (z.B. Betriebssystem von Tablets und PC und den installierten Software-Paketen)
- Wer ist für den Betrieb der Komponenten (Firewall, Webpräsenz, Telefonanlage, Fileserver etc.) verantwortlich und mit welchen Erreichbarkeiten?
- Welche Regeln für eingehende und ausgehende Verbindungen sind auf der Firewall hinterlegt? Sind diese noch notwendig und aktuell?
- Welche Daten liegen bei externen Anbietern bzw. in einer Cloud? Wie ist dieser Anbieter erreichbar, sind die Daten dort ausreichend sicher hinterlegt (verschlüsselt)?
- Wer ist IT-Dienstleister mit welchen Zugriffsmöglichkeiten und Kontaktdaten?
- Sind die u.U. im Einsatz befindlichen Händlerkonten bei eBay oder Amazon ausreichend dokumentiert?

Sonstiges:

Eine Dokumentation kann schnell einen hohen Arbeitsaufwand erfordern ist aber unersetzlich. Der Nutzen der Dokumentation kommt meist bei auftretenden Problemen zu Tage oder sobald wissenstragende Personen das Unternehmen verlassen.

Vereinfachen kann man die Dokumentation z.B. mit Konfigurationsverwaltungstools oder technisch über Managementschnittstellen der Geräte. In Verbindung mit dem Change-Management, unter Punkt 5 erklärt, ergibt sich so ein kompletteres Bild der Infrastruktur

und der derzeitigen Einstellungen.

Nur wenn man die eigene IT-Infrastruktur kennt kann man Bedrohungen und Schwachstellen und die daraus resultierenden Risiken effektiv erkennen und beurteilen.

5. Change-Management

Änderungen an der Infrastruktur, an den Benutzern oder z.B. den Firewallregeln sollte festgehalten werden und somit nachvollziehbar sein.

Beispiele:

- Ein neues Rechnersystem wird aufgestellt oder entfernt
- Ein Port wird in der Firewall freigeschaltet, Dokumentation inklusive des Zwecks dieser Freischaltung (z.B. Wartung durch Externe)
- Fernzugriffsmöglichkeiten über Teamviewer oder VPN dokumentieren
- Wiedervorlage und Prüffristen einbauen
- Gleiches gilt für besondere Berechtigungen an Benutzern oder Freigaben für spezielle Ordner
- Die dokumentierten Änderungen können für den Prozess "Mitarbeiter verlässt das Unternehmen" sehr hilfreich sein.

Sonstiges:

Das Change-Management ist auch hilfreich für die Abschätzung der Folgen einer Änderung in der IT-Infrastruktur. Relevant zum Beispiel für den Fall eines dringend notwendigen Changes.
Beispiel: Es müssen aufgrund einer bekanntgewordenen Schwachstelle dringend Maßnahmen zur Reduzierung einer möglichen Ausnutzung eingeleitet werden.

Für eine solche Abschätzung wird eine gute Dokumentation, wie im Punkt Dokumentation beschrieben, benötigt.

6. Prozesse

Die Festlegung der Prozesse für unterschiedliche Fälle sind wichtig. Eine Person verlässt das Unternehmen, ein interner Wechsel zu einer anderen Abteilung oder auch die Freigabe einer Software seien hier als Beispiele genannt.

Beim Verlassen des Unternehmens sind zum Beispiel folgende Dinge festzulegen:

- Daten des Benutzers archivieren/sichern/löschen
- Fileserver-Konto löschen bzw. Zugriff entziehen

- E-Mailadresse inaktiv schalten/umleiten bzw. entfernen
- Welche Passwörter sind dem Nutzer darüber hinaus noch bekannt? Denken Sie beispielsweise an die Passwörter für WLAN-Netze, extern genutzte E-Mailkonten oder z.B. ein Verkäuferkonto bei eBay oder Amazon
- Zugangsmöglichkeiten zu Gebäuden entziehen

Bei einem internen Wechsel ist darauf zu achten, dass nicht mehr benötigte Berechtigungen entfernt werden um eine Anhäufung von nicht mehr benötigten Berechtigungen zu vermeiden.

Je nach Firmengröße kann ein Freigabeprozess für Software kann sinnvoll sein. So können MitarbeiterInnen für die Arbeit nützliche Software verwenden aber bevor dies geschieht wird geprüft ob die Software sicher ist:

- Wer darf Software zur Nutzung freigeben? - Hier bietet sich z.B. einer mehrstufige Kontrolle an mit Blickwinkel aus der rechtlichen, technischen und sicherheitstechnischen Sicht.
- Wird die Software bentötigt? Gibt es bereits eine Software im EInsatz die den Funktionsumfang bietet?
- Welchen Lizenz-und Nutzungsrechten unterliegt die Software - eine Freeware ist häufig nur für nicht-kommerzielle Nutzung kostenfrei verwendbar
- Verfügt die Software über eine aktive Wartung/Entwicklung z.B. zur Schließung von Sicherheitslücken
- Erlaubt die Software Fernzugriff/Öffnet Sie zusätzlich Verbindungen zum Internet?

7. Passwörter und Benutzerzugänge

Für Kennwörter müssen besondere Regeln gelten:

- Kennwörter müssen pro Benutzer schon bei der Vergabe einmalig und hinreichend komplex sein.
- Kennwörter sollten regelmäßig geändert werden.
- Die Zugänge von Mitarbeitern, die das Unternehmen verlassen, müssen gelöscht bzw. unbrauchbar gemacht werden.
- Das Hinterlegen von Kennwörtern beispielsweise in Anmeldeskripten sollte vermieden werden.
- Die Hinterlegung von Kennwortlisten auf Dateiservern sollte nicht praktiziert werden.
- Es gibt sogenannte Passwort-Manager, die bei der Verwaltung von Passwörtern helfen.
- Kennwörter können an einem sicheren Ort hinterlegt werden (Tresor).
- Für jeden Zweck sollte ein eigenes Kennwort verwendet werden.
- Sichere Authentifizierungsverfahren (2-Faktor Authentifizierung) sollten verwendet werden.
- Technische Maßnahmen zur Anbindung an die Infrastruktur (SSO mittels SAML, Kerberos, OAuth etc.)
- Ein Benutzerzugang sollte nicht von mehreren Benutzern gemeinsam genutzt werden (beispielsweise das Login bei Handelsplattformen).

Sonstiges:

NutzerInnen sollten nur so viele Berechtigungen zugeteilt bekommen, wie sie für die Erfüllung ihrer Aufgaben tatsächlich benötigen - das beinhaltet insbesondere den Zugriff auf Datei-Freigaben.

Power-User und AdministratorInnen sollten über mehrere Accounts, z.B. normale Berechtigungen und erweiterte Berechtigungen, verfügen um ein unnötig durchgehendes Arbeiten mit erweiterten Rechten unnötig zu machen.

8. Backup

Im Hinblick auf alle Bedrohungen ist ein Backup von grundlegender Bedeutung. Sei es nun ein Hardwareschaden, eine Malware-Infektion oder ein Löschen von Daten durch BentuzerInnen.

<u>Dabei sollten die folgenden Punkte geprüft bzw. beachtet werden:</u>

- Das Backup muss regelmäßig erstellt werden, am Besten automatisiert
- Es ist eine Historisierung anzuwenden
- Die Backup-Medien müssen regelmäßig geprüft werden
- Es muss über fehlgeschlagene Backups benachrichtigt werden
- Das Backup-Medium darf nicht online immer am Netzwerk/Server hängen
- Es sind auch Backup-Medien außerhalb der Firmenräume zu lagern (Beispiel: Brand in den Firmenräumen)
- Die Wiederherstellung muss regelmäßig erprobt werden
- Rechtliche Eckpunkte bzgl. wie lange darf oder muss ich die Verfügbarkeit von Daten sicherstellen - hierbei kann auch über eine Archivierung nachgedacht werden

Sonstiges:

Denken Sie beim Thema Backup nicht nur an eine Kopie Ihrer Daten! Beachten Sie nach Möglichkeit auch eine Redundanz von IT-Systemen, die von zentraler Bedeutung sind (Ersatz von Hardware, Failover-Systeme).

9. Software und Updates

Das Einspielen von aktuellen Software-Versionen ist Grundlage für einen sicheren Betrieb der IT.

<u>Das betrifft alle Komponenten, beispielsweise:</u>

- Server

- Clients
- Virenscanner inklusive Signaturen
- Router, Switche
- Telefonanlagen
- Webserver mit verwendetem CMS-System (z.B. Wordpress inklusive Plugins)

Sonstiges:

Software auf den Clients, die nicht unbedingt benötigt wird, sollte deinstalliert werden.

Eine Überwachung auf die Betroffenheit von veröffentlichten Schwachstellen z.b. über öffentliche Quellen sollte erfolgen. Wenn eine eingesetzte Software von einer Schwachstelle betroffen ist aber noch kein Update vorhanden ist sollte passend zum Risiko über andere Maßnahmen nachgedacht werden.

10. Netzwerksicherheit

Bei der Gestaltung des Netzwerkes (Kabel oder auch Funk) beachten Sie die folgenden Hinweise:

- Trennen Sie Netze mit unterschiedlichen Aufgaben voneinander und implementieren sie Kontrolmechanismen an den Netzübergängen
- Vernetzen Sie nach Möglichkeit keine Komponenten, die für einen Netzwerkbetrieb nicht ausgelegt waren/sind
- Prüfen Sie bei jedem Gerät welche Schnittstellen/Ports nach außen geöffnet werden und ob ggf. eine automatische Freischaltung von Ports erfolgt
- Kontrollieren Sie regelmäßig die auf der Firewall eingerichteten Portfreigaben
- Schaffen Sie ggf. die Möglichkeit, Netzwerksegmente kurzfristig zu separieren und so eine Ausbreitung von beispielsweise Schadsoftware zu verhindern
- Regeln Sie die Nutzung von privaten IT-Geräten, die ggf. in das Firmennetz eingebunden werden
- Gibt es die Möglichkeit, aus der Ferne auf das Netzwerk zuzugreifen? Sind diese Zugänge ausreichend abgesichert (z.B. via VPN)?
- Verwenden Sie bei WLAN-Zugängen starke Verschlüsselung und sichere Passwörter
- Separieren Sie WLAN-Netze von Produktivumgebungen- soweit möglich
- Je nach Größe Ihres Netzwerks sollten Sie unterschiedliche Sicherheitslösungen und mehrere Ebenen der Mechanismen einführen (Defense-in-Depth) um es Angreifern möglichst schwer zu machen un Schwächen in den Sicherheitslösungen auszugleichen.

Phänomene und Angriffsszenarien

Hier bekommen Sie einen Eindruck, welche Gefahren Ihrem Unternehmen im täglichen Leben drohen und wie Sie sich davor schützen können. Darüber hinaus enthält diese Aufstellung auch erste Maßnahmen nach einem Angriff.

Die Hinweise sind nicht abschließend, sondern decken nur die häufigsten Angriffe im Internet und mögliche Maßnahmen ab.

Die hier aufgeführten Maßnahmen sind nach Phänomenen in präventive, detektive und reaktive (Notfall-) Maßnahmen unterteilt:

- Präventive Maßnahmen mit dem Ziel der Reduzierung der Eintrittswahrscheinlichkeit und der Verringerung des Ausmaßes bei Eintritt,
- Detektive Maßnahmen mit dem Ziel der möglichst frühzeitigen Erkennung von Angriffen,
- Reaktive bzw. Notfallmaßnahmen mit dem Ziel der Eingrenzung und Behebung von Schäden sowie die Wiederherstellung des Betriebes.
  Besprechen Sie die Hinweise und Fragen mit Ihrem IT-Dienstleister. Bei entsprechender Kompetenz wird er auskunftsfähig sein und Ihre Fragen beantworten können.

1. Ransomware/Verschlüsselungstrojaner

Ziel eines Verschlüsselungtrojaners ist es Dateien und Systeme des Opfers zu verschlüsseln, um Lösegeld für ihre Entschlüsselung zu verlangen.
Die Verschlüsselung an sich ist häufig der letzte Schritt und wird erst ausgeführt, nachdem eine weite Ausbreitung im Netzwerk erfolgt ist. Dies führt zu einer Maximierung des Schadensausmaßes für die betroffenen Opfer.
Moderne Varianten dieser Bedrohung leiten zusätzlich Daten aus. Hintergrund ist ein weiteres Druckmittel, um Geld von Opfern zu erpressen, da diese eine Veröffentlichung der Daten verhindern wollen.

Haupteinfallstore für eine Infektion und weitere Ausbreitung sind:

- Ausführung eines schadhaften E-Mail-Anhangs
- Herunterladen und Ausführen von Schadsoftware beim Surfen im Internet
- Ausnutzung von Schwachstellen, Konfigurationsfehlern und/oder geknackten/geleakten Zugangsdaten in extern verfügbaren Schnittstellen (VPN, Fernwartung)

Präventive Maßnahmen

- Filterung und Scan auf dem Mail-Gateway/beim Provider
- Aufbau von Vertrauen in den Absender von E-Mails mit Hilfe von Signaturen
- Rückfrage über zweiten Kommunikationskanal beim Versender
- Schulung von Mitarbeitern (Awareness, Wissen um die Bedrohungen)
- Härten der Systeme (Endpoints, Server, Gateways, Applikation)

        - Blockieren von Windows-Scripting-Host
        - Blockieren von Makros in Office-Dokumenten
        - Festlegen einer Whitelist für Dateianhänge
    - Netzwerksegmentierung
        - Trennung nach Aufgabengebiet und/oder Datenklasse
        - Spezielle Netze für offenen Internetzugang und Gäste
    - Festlegen von Ansprechpartnern bei „Grenzfällen“
    - Sicherung Ihrer Daten und Systeme - sehen Sie hierzu auch unsere Präventionsmaßnahmen zum Thema Backup
    - Erstellung eines Notfallplans für den Fall einer Infektion - sehen Sie hierzu auch unsere empfohlenen Präventionsmaßnahmen zu Notfallplänen

Detektive Maßnahmen

- Aktives Monitoring der Meldungen von Anti-Threat-Software
- Einsatz von Host Intrusion Detection Systemen (HIDS)
- Einsatz von Network Intrusion Detection Systemen (NIDS)
- Monitoring von Netzwerkaktivitäten und Dateizugriffen mit entsprechenden Regeln
- Monitoring der Ausführung von unbekannten Programmen mit administrativen Rechten
- Meldungen von Usern zu auffälligen Mails/Meldungen auf IT-Systemen

Notfallmaßnahmen

- Betroffene Systeme identifizieren und vom Netz trennen
- Ausmaß feststellen - Welche Daten/Systeme sind betroffen? Wiederherstellung möglich? Wenn ja, welcher Aufwand?
- Behörden einbinden/informieren -> Polizei, Datenschutzbehörde
- Versicherung einbinden - wenn vorhanden
- Ggf. externe Dienstleitungsunternehmen zur Unterstützung einbinden (siehe BSI-Liste APT-Response-Dienstleister)
- Kommunikation - Koordination, was und wann an welche Stellen kommuniziert werden soll:
    - Interne Kommunikation an MitarbeiterInnen
    - Externe Kommunikation an KundInnen
    - Externe Kommunikation an Presse
- Attack Chain feststellen - Wie kam es wann auf welchem System zur Infektion?
- Recherche, diese Daten erhalten Sie mitunter auch von uns:
    - Um welche Ransomware handelt es sich? Welche Tätergruppierung steckt dahinter?
    - Gibt es Informationen über Entschlüsselungsmöglichkeitenm?
    - Bekannte Erfahrungen zum Verhalten bei Zahlung von Lösegeldsummen?
- Eigene Entscheidungen treffen anhand des Ausmaßes:
    - Muss eine Lösegeldsumme gezahlt werden?
    - Muss Kontakt mit den TäterInnen aufgenommen werden?

- Säubern der Systeme
- Wiederherstellen der Funktionsfähigkeit der Systeme

2. CEO-Fraud & BEC (Business E-Mail Compromise)

Ziel des Angriffs ist es durch das Vorgeben einer gefälschten Identität eine Überweisung von hohen Geldbeträgen zu erreichen oder eine richtige Rechnung auf eine gefälschte Bankverbindung umzuleiten.
Als gefälschte Identität werden bevorzugt Geschäftspartner und in der Hierarchie weit oben liegende Personen genutzt, z.B. die Geschäftsführung.

Die Angriffsmethoden lassen sich in zwei Varianten einteilen:

Variante 1:
Täter melden sich auf einem Kommunikationsweg (E-Mail, Anruf) in der Buchhaltung einer Firma und versuchen durch geschickte Gesprächsführung eine Zahlung zu initiieren. Die Täter geben sich dabei zum Beispiel als Geschäftsführer aus und verwenden Vertraulichkeitsklauseln oder vermeintliche Vorgaben der Bafin, um den Empfänger zu manipulieren.

Variante 2:
Beim sogenannten Business E-Mail Compromise verändern Täter entweder beim Versender, auf dem Versandweg oder beim Empfänger eine Rechnung oder Mahnung und versuchen damit die Zahlung auf ein eigenes Konto umzuleiten. Durch die verwendete Gesprächsführung wird die Notwendigkeit einer Kontoänderung plausibel gestaltet. In anderen Fällen werden Rechnungen für fiktive Produkte erstellt und die Firmen so zu einer Zahlung gebracht.

Die beiden Varianten unterscheiden sich darin, dass bei der Variante 2 ein Zugriff auf die vorhandene Kommunikation notwendig ist.

Präventive Maßnahmen

- Rückfrage über einen zweiten Kommunikationskanal beim Versender
- Schulung von Mitarbeitern (Awareness, Wissen um die Bedrohungen)
- Offene Kommunikation im Unternehmen und mit Geschäftspartnern, vertrauensvolle Zusammenarbeit
- Verwendung von Verschlüsselung und Signatur für die geschäftliche und interne Kommunikation via E-Mail
- Konfiguration des Mailprogramms, um den Absender einer E-Mail und die Quelle einwandfrei identifizieren zu können (Antwort-An Adresse als Spalte einblenden)
- Nutzung sicherer Passwörter und Mehrfaktorauthentifizierung bei E-Mailkonten
- Zugang aus dem Internet auf die E-Mails unterbinden - z.B. Zugang nur intern oder über VPN
- Anzeige im Mail-Programm, damit E-Mails von extern oder von nicht bekannten

Adressen explizit als solche ausgewiesen werden

Detektive Maßnahmen

- Monitoring der (versuchten) Anmeldungen an Mail-Konten

Notfallmaßnahmen

- Versuchen Sie umgehend über Ihr Geldinstitut eine Rückbuchung der gezahlten Gelder zu erwirken. Nehmen Sie umgehend Kontakt zur Polizei zwecks Rückholung auf!
- Prüfen Sie, ob ein Zugriff auf Ihre Systeme (Mail-Konten) erfolgt ist. Ergreifen Sie, wenn ja, entsprechende Maßnahmen
  - Ändern der Zugangsdaten
  - Prüfen ob weitere E-Mails versendet wurden
  - Eventuell Kontaktaufnahme zu weiteren Empfängern um diese zu warnen
  - Wenn es zu einer Kompromittierung gekommen ist, kann eine Meldung bzgl. Datenschutz notwendig sein
- Wenn eine manipulierte E-Mail von einem bekannten Geschäftspartner kam, ist dieser darüber in Kenntnis zu setzen

3. TK-Hacking

Unter TK-Hacking versteht man das unberechtigte Verwenden von Telefonanlagen, um über das Anwählen von teuren Mehrwertnummern einen Gewinn zu erzielen. Dabei werden in der Regel Fernwartungs- oder Fernnutzungszugänge verwendet, die entweder gar nicht oder schlecht geschützt sind.

Präventive Maßnahmen

- Mit dem Dienstleister klären ob ein Fernzugriff und in welcher Form eingerichtet ist
- Abschaltung des Fernwartungszugriffs und/oder des Fernnutzungszugriffs
- Absichern des Fernwartungszugriffs und/oder des Fernnutzungszugriffs
  - Nutzung sicherer Passwörter und Mehrfaktorauthentifizierung
  - Nutzung von VPN für den Zugriff
- Regelmäßige Updates der TK-Anlage - Softwarestand aktuell halten
- Sperren von kostenpflichtigen Service-Nummern und Auslandsrufnummern

Detektive Maßnahmen

- Monitoring der (versuchten) Anmeldungen/Zugriffe
- Monitoring der ausgehenden Rufe

Notfallmaßnahmen

- Provider über den Missbrauch informieren
- Ändern/Absichern der Zugänge zur TK-Anlage
- Säubern der TK-Anlage, hierzu zählt mitunter die Wiederherstellung der korrekten Konfiguration

4. DB-Hacking bzw. Web-Defacing

Unter diesen Begrifflichkeiten zusammengefasst fallen alle Einwirkungen auf die Webpräsenz oder das Unternehmensnetzwerk mit der Folge des Auslesens, des Zerstörens oder der Manipulation von Inhalten.

Häufig genutzte Angriffswege:

- Ausnutzung von Schwachstellen in mitunter veralteter Software
- Nutzung von geleakten/geklauten Zugangsdaten
- Knacken von Einfachstpasswörtern simplen Zugangsdaten

Beispiele für Manipulationen:

- Ihre Webseite verteilt Schadsoftware an die Besucher
- Die Datenbanken der Webseiten werden ausgelesen und Sie werden damit erpresst oder die Daten gelangen in falsche Hände
- Die Täter legen illegale Inhalte auf Ihrem Webserver ab
- Die Täter platzieren eine Phishing-Seite auf Ihrem Server
- Die Täter nutzen Ihren Server zum Generieren von Kryptowährung (sog. Bitcoin-Mining)
- Täter verändern den Inhalt Ihrer Webpräsenz um Ihrem Image zu schaden

Präventive Maßnahmen

- Regelmäßige Updates der Datenbankmanagementsysteme, Webserver, Content Management Systeme und deren Apps - Softwarestände aktuell halten
- Absichern der Nutzer und Admin-Zugriffe
- Bei Eigenentwicklungen - Secure Coding und Qualitätssicherung
- Einsetzen einer Web Application Firewall um Angriffe über z.B. SQL Injection oder Cross-Site-Scripting abzufangen
- Trennen der Webinhalte auf verschiedene Systeme nach Inhalt und Zweck (Intranet, Internet)
- Einführung bzw. Nutzung von 4-Augen-Prinzip um eine Freigabe neuer Webinhalte durch eine einzelne Person/einen einzelnen Account zu verhindern

Detektive Maßnahmen

- Regelmäßiges Prüfen von veröffentlichten Webinhalten
- Monitoring der Logins von Usern/Administratoren
- Monitoring der ausgeführten SQL-Befehle

Notfallmaßnahmen

- Ändern/Absichern der Zugänge
- Ggf. Offline-Nehmen der betroffenen Services
- Identifizieren der Manipulationen und des Ausmaßes
- Säubern der Systeme/Wiederherstellen der Konfiguration
- Ggf. Meldung an Datenschutz

5. (D)DoS

Ein (D)DoS-Angriff dient dazu Netzwerke, Server und/oder Dienste unverfügbar/unnutzbar zu machen.

Es muss daher eine Einschätzung getroffen werden, welche Bereiche tangiert sein können und welche Auswirkungen eine Attacke haben könnte. Wird festgestellt, dass ein Lahmlegen der Webseite (z.B. inklusive Shopsystem) zu einem immensen Verlust führen würde, sind Maßnahmen schon im Vorfeld mit dem Provider zu besprechen wie auf einen solchen Angriff reagiert werden kann oder wie die Gefahr dafür im Vorfeld minimiert werden kann.

Ein Angriff kann mitunter Folgendes betreffen:

- Nichterreichbarkeit von Internet-Services (Web-Shop, Web-Page)
- Störung von Mail-Servern, VPN-Zugängen, SIP-Servern (VoIP)
- Zusätzlich Lösegeldforderung um den Angriff zu beenden

Präventive Maßnahmen

- Server-Härtung (mitunter Deaktivierung von unnötigen Diensten, aktuellste Patches)
- Netzwerksegmentierung
- Auslagerung von besonders exponierten Systemen
- Nutzung von speziellen DDoS-Mitigations-Dienstleistern/-Technologien (siehe: BSI-Liste)
  - DDos-Mitigation-Appliance
  - Content Delivery Networks
  - DDos-Mitigation-as-a-Service
- Zusätzliche Ressourcen vorhalten

Detektive Maßnahmen

- Monitoring der System-Auslastung
- Monitoring der Zugriffszahlen
- Monitoring des Netzwerktraffics

Notfallmaßnahmen

- Ausmaß feststellen
- Herkunft feststellen

- Netzwerksegmentierung
- Auslagerung von besonders exponierten Systemen
- Rücksprache mit ISP/DDOS-Mitigation-Service-Provider
- Kommunikation - Entscheidung was und wann an welche Stellen kommuniziert werden soll:
    - Interne Kommunikation an MitarbeiterInnen
    - Externe Kommunikation an KundInnen
    - Externe Kommunikation an Presse
- Filterung (Blackholing, Sinkholing)

6. Phishing und Scamming

Unter Phishing und Scamming fallen Angriffe, die den Menschen/User direkt betreffen.
Phishing hat hierbei das Ziel Daten zu erlangen während Scamming das Ziel hat Geld zu erlangen. Als Methode kommen häufig gefälschte Rufnummern und E-Mail-Adressen zum Einsatz, welche den Opfern eine vertrauenswürdige Identität vortäuschen sollen.

<u>Folgende spezifische Phänomene sind hier mitunter bekannt:</u>

- MS-Support-Scam - ein angeblicher Microsoft-Support-Mitarbeiter ruft an wegen eines angeblichen Virenbefalls Ihres Computers. Ziel ist es, eine Überweisung von hohen Geldbeträgen auf ein fremdes Konto zu erwirken.
- Der CEO-Fraud (siehe **CEO-Fraud**) ist eine Variante eines gezielten Scams.

Generell gibt es die unterschiedlichsten Varianten von Phishing/Scamming. Die Tätergruppen agieren hier kreativ und probieren immer wieder mit neuen Varianten in abgewandelter Form ihre Opfer zu täuschen.

Präventive Maßnahmen

- Schulung von Mitarbeitern (Awareness, Wissen um die Bedrohungen)
    - E-Mail-Adressen und Telefonnummern können gefälscht sein
    - Über Telefon/Internet kann sich jeder als jede beliebige Person ausgeben
    - Aufklärung wie der IT-Support sich authentifizieren kann
- Rückfrage über zweiten Kommunikationskanal
- Links in Mails nicht folgen sondern die Zielseite (z.B. PayPal) selber im Browser aufrufen und einloggen
- Fernzugriffsmöglichkeiten auf Endpunkten (z.B. TeamViewer/AnyDesk/MS RDP) absichern/deaktivieren

Detektive Maßnahmen

- Anzeige im Mail-Programm wo eine Mail herkommt (z.B. Absender IP-Adresse in

fremdem Land, Absender eigentlich aus Deutschland)
- Rückfrage über zweiten Kommunikationskanal
- Links in Mails nicht folgen sondern die Zielseite (z.B. PayPal) selber im Browser aufrufen und einloggen
- Fernzugriffsmöglichkeiten auf Endpunkten (z.B. TeamViewer/AnyDesk/Microsoft RDP) absichern/deaktivieren
- Meldungen von Usern zu auffälligen Mails/Meldungen auf IT-Systemen
- Überwachung von Leakseiten

Notfallmaßnahmen

- Wenn Sie/ein User auf einen Phishing-Versuch hereingefallen sind, ändern Sie alle betroffenen Zugangsdaten
- Bei einer getätigten Überweisung kontaktieren Sie schnellstmöglich Ihr Finanzinstitut

7. Spam-Versand über den Firmen-Mailserver

Alle Systeme, die vom Internet aus verfügbar sind, können potentiell missbräuchlich verwendet werden. Unter anderem ist dies bei der Firmen-Webseite (siehe DB-Hacking) denkbar, aber auch bei dem eingesetzen Mailsystem. Es sind verschiedene Varianten denkbar, wann ein Missbrauch eines Mailsystem möglich wird:

Folgende Varianten sind hier bekannt:
- Ausnutzung einer Fehlkonfiguration (Stichwort Open-Relay)
- Nutzung von geleakten/geklauten Zugangsdaten
- Knacken/Erraten von simplen Zugangsdaten
- Ausnutzung von Schwachstellen in mitunter veralteter Software

Präventive Maßnahmen

- Halten Sie Ihre Mail-Server aktuell
- Nutzen Sie eine gehärtete Konfiguration
- Sichere Passwörter und Mehrfaktorauthentifizierung bei E-Mailkonten
- Prüfen/Testen Sie auf mögliche Schwachstellen

Detektive Maßnahmen

- Protokollierung und Monitoring von empfangenen/versendeten Mails
- Überwachen von Leakseiten

Notfallmaßnahmen

- Ermittlung des verwendeten Benutzerkontos und Änderung von Passwörtern/Deaktivierung des Kontos
- Feststellen der ausgenutzten Konfigurationslücke und Behebung dieser
- Kommunikation - Entscheidung was und wann an welche Stellen kommuniziert

werden soll:
    - Interne Kommunikation an MitarbeiterInnen
    - Externe Kommunikation an KundInnen
    - Externe Kommunikation an Presse
- Identifizieren der Manipulationen und des Ausmaßes
- Säubern der Systeme/Wiederherstellen der Konfiguration
- Ggf. Meldung an Datenschutz