ZAC-Nds. - Präventionsmaßnahmen und Angriffsszenarien

Stand der Präventionshinweise: 03.04.2021 17:12 Uhr

Stand der Angriffsszenarien: 07.05.2019 14:14 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.

<u>Fragen, die in diesem Zusammenhang zu stellen sind:</u>

- 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 die ersten Maßnahmen nach einem Angriff.

Die Hinweise sind jeweils nicht abschließend, sondern decken nur die wichtigsten Angriffe im Internet ab.

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

1. Ransomware/Verschlüsselungstrojaner

Durch eine Schadsoftware werden die lokalen Daten des infizierten PC und ggf. die eingebundenen Netzfreigaben verschlüsselt. Varianten von Ransomware verbreiten sich danach von Rechner zu Rechner.

Zu den gängigsten Infektionswegen gehören:

- Infektion durch Ausführen eines schadhaften E-Mailanhangs
- Infektion durch „Drive-By“, d.h. das Surfen im Internet
- Infektion durch Aufschalten per Fernwartungssoftware

1.1 Infektion durch Ausführen eines schadhaften E-Mailanhangs

Vorbeugung für diese Art der Infektion können die folgenden technischen Maßnahmen sein (Achtung: Nie 100%-Schutz):

- Filterung und Scan auf dem Mail-Gateway/beim Provider
- Aufbau von Vertrauen in den Absender von E-Mails mit Hilfe von Signaturen
- Blockieren von Windows-Scripting-Host
- Blockieren von Makros in Office-Dokumenten
- Einsatz von alternativen Office-Produkten
- Einsatz von alternativen PDF-Produkten
- Einsatz von Linux auf den Clients

Organisatorische Maßnahmen:

- Schulung von Mitarbeitern (Awareness, Wissen um die Bedrohungen)
- Festlegen einer Whiteliste für Dateianhänge
- Festlegen von Ansprechpartnern bei „Grenzfällen“
- Rückfrage beim Versender

1.2 Infektion durch sog. „Drive-By“- dem Surfen im Internet

Das bloße Aufrufen einer Internetseite kann zur einer Infektion mit Schadsoftware führen.

Die folgenden technischen Maßnahmen können die Infektion verhindern oder das Risiko für eine Infektion verkleinern:

- Deaktivierung von Flash/Java und nicht verwendeten Plugins im Browser
- Einsatz von alternativen Browsern z.B. Firefox
- Virenschutz auf dem Gateway
- Virenschutz auf dem Client
- Einsatz eines Proxies mit gesonderter Authentifizierung
- Führen einer Whitelist für den Aufruf von Internetseiten
- Einrichten von Arbeitsplätzen, getrennt vom Unternehmensnetzwerk, für das Surfen im Internet
- Kein privater Internetgebrauch im Unternehmensnetz

1.3 Infektion durch die Ausnutzung von Fernwartungsprogrammen

Täter scannen im Internet nach offenen Zugängen zur Administration von Netzwerken bzw. Lesen Kennwörter von administrativen Fernzugängen aus. Danach schalten sie sich auf die System und verschlüsseln die Systeme, um dann einen bestimmten Betrag für die Freigabe der Daten zu erpressen.

Die folgenden technischen Maßnahmen können die Gefahr einer Ausnutzung von Fernwartungsprogrammen verkleinern.

- Erhebung der bestehenden Fernzugänge
- Ggf. Deaktivierung von Fernwartungszugängen
- Ggf. Deaktivierung von Netzzugängen z.B. via WLAN
- Verwendung von sicheren Fernwartungsprogrammen (optimal: via VPN, ggf. auch Produkte wie Teamviewer)
- Kein Einsatz von unverschlüsselten Fernwartungsprogrammen
- Deaktivierung und Entfernung von inaktiven und alten Benutzeraccounts
- Keine Passwörter im Klartext, z.B. in Skripten auf den Clients oder Servern (Beispiel: Anmeldeskripte auf Windows-Systemen i.Z.m. „net use“)

Maßnahmen bei Feststellung einer Verschlüsselung:

- Ermittlung des Infektionsweges
- Ermittlung des auslösenden Rechners und Runterfahren dieses Systems
- Wiederherstellung von Daten aus dem Backup (siehe **Backup**)
- Regeln erstellen, um erneutes Eindringen bzw. Auslösen zu verhindern
- Alle Systeme im Netzwerk auf Befall prüfen
- Benachrichtigung aller Benutzer über den Infektionsweg

2. CEO-Fraud & BEC

Gemeint ist hier der Fall, dass Täter sich als CEO oder sonstiger Bevollmächtigter einer Firma ausgeben und Aktionen bei ahnungslosen Mitarbeitern auslösen.

Es kann dabei eine der folgenden Varianten zum Einsatz kommen:

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 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.

Es gibt sowohl technische als auch organisatorische Maßnahmen, um diese Form der Manipulation nicht wirksam werden zu lassen.

Technische Maßnahmen:

- Verwendung von Verschlüsselung und Signatur für die geschäftliche, interne Kommunikation via E-Mail
- Konfiguration von Outlook, um den Absender einer E-Mail und die Quelle einwandfrei identifizieren zu können (Antwort-An Adresse als Spalte einblenden)
- Sichere Passwörter bei E-Mailkonten
- Ist ein Zugang zum Mailsystem von außerhalb möglich bzw. erforderlich? (z.B. Outlook Web-Access)
- Können E-Mails von außerhalb mit der Firmen-Mailadresse in die Firma gesendet werden?

Organisatorische Maßnahmen:

- Schulung der Mitarbeiter
- Vier-Augen-Prinzip
- Offene Kommunikation im Unternehmen, vertrauensvolle Zusammenarbeit
- Rückfrage auf einem alternativen Kommunikationsweg

Erste Maßnahmen wenn es zu einem Schaden gekommen ist:

- Versuchen Sie umgehend über Ihr Geldinstitut eine Rückbuchung der gezahlten Gelder zu erwirken

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.

Die folgenden Maßnahmen können eine Missbrauchsgefahr verringern:

- Klärung: Besteht ein Fernwartungszugang??
- Wie ist der Zugang geschützt? Gibt es Standard-Passwörter?
- Wie kann die Fernwartung sicher gestaltet werden (u.U. Einsatz eines VPN)?
- Kann die TK-Anlage von außen verwendet werden, sind die Passwörter sicher??
- Wird die TK-Anlage aktuell gehalten? Wer kümmert sich um die Updates?

4. DB-Hacking

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

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 wollen dem Image Ihres Unternehmens schaden und verunstalten daher die Seite

Die folgenden Dinge sind bei der eigenen Webseite zu berücksichtigen:

- Gibt es eine Unternehmenswebseite?
- Was ist der Inhalt? Ist die Verwendung von weniger verwundbaren statistischen Seiten möglich?
- Wird das verwendete CMS-System aktuell gehalten und inklusive der Plugins mit Updates versorgt?
- Wird eine verschlüsselte Verbindung angeboten?
- Ist die Webseite auf die Standard-Angriffe wie SQL-Injection und Cross-Side-Scripting geprüft?
- Wird der Zugriff auf die Webseite protokolliert und von Zeit zu Zeit geprüft?
- Wird die Webseite regelmäßig auf Veränderungen geprüft?

5. DDOS

Unter DDOS versteht man das Lahmlegen von Netzwerken oder Servern durch eine Flut von Anfragen. Auch große Firmen sind regelmäßig betroffen. Wirksame Schutzmechanismen sind aufwändig und teuer.

Es muss daher eine Einschätzung getroffen 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.

Maßnahmen könnten hier sein:

- Gespräch mit dem Provider wie im Angriffsfall reagiert wird (Abschaltung, Umleitung, Verteilung, Blockieren)
- Verwendung von DDOS-Schutzeinrichtungen (Cloudflare etc.)
- Feststellung, dass die Webseite nur Visitenkarte ist und keine Maßnahmen erforderlich sind
- Bewertung von Androhungen ob es sich um eine reale Gefahr oder um Trittbrettfahrer handelt

6. Phone-Scam bzw. MS-Support Anrufe

Täter geben sich am Telefon als Mitarbeiter von Microsoft oder einer anderen Firma aus und versuchen die angerufene Person zu einer Aktion zu bringen. Das kann z.B. das Auslösen einer Überweisung, die Installation einer Software oder die Einrichtung einer Fernwartung sein.

Ein wirksamer Schutz ist durch Aufklärung der Mitarbeiter und Kommunikation der berechtigten IT-Supportfirmen an die Mitarbeiter möglich.

7. Spam-Versand über den Firmen-Mailserver

Alle Systeme, die von einer Firmen in das Internet eingebunden sind, können 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:

- Bei einer falschen Konfiguration des Systems (Stichwort: Open-Relay, d.h. jeder kann über Ihr System E-Mails an beliebige Empfänger versenden)
- Bei der Verwendung von schwachen Kombinationen von Benutzername und Kennwort bei der Authentifizierung für das Senden von E-Mails

Gegenmaßnahmen:

- Halten Sie sich an die Hinweise unter **Passwörter und Benutzerzugänge**, um den Zugang mit schwachen Zugangsdaten zu erschweren
- Testen Sie Ihr Mailsystem auf die unberechtigte Verwendbarkeit durch Dritte
- Protokollieren Sie den Empfang und Versand von E-Mails, um Missbrauch zu detektieren
- Prüfen Sie E-Mail Rückläufer, um Missbrauch zu entdecken

Maßnahmen bei Feststellung eines Missbrauchs:

- Ermittlung des verwendeten Benutzerkontos und Änderung von Passwörter/Deaktivierung
- Feststellen der ausgenutzten Konfigurationslücke und Behebung dieser
- Benachrichtigung von Empfängern der missbräuchlich gesendeten E-Mails