IT-Sicher
im Netz(werk) unterweg

Unternehmerinnen Forum Niederrhein

17. März 2021

Jessica Saum, CommuniBIT e.K.

www.communibit.com

Übergeordnetes Ziel

- Datensicherheit
  - Vertraulichkeit
  - Integrität und
  - Verfügbarkeit der Daten
- Datensicherheit ist gefährdet durch
  - technische Mängeln
  - fremder Zugriff auf die Daten

IT-Sicherheit / Cyber Security

- Technischer Störfall
  - Störung des bestimmungsgemäßen Betriebs (Systemfehler, Ausfälle)
- IT-Sicherheitsvorfall
  - Ungesetzliche, nicht autorisierte bzw. unerwünschte Handlung

- Die Bedrohungslage wird unterschätzt
  - In 28 Prozent der Unternehmen gab es in den letzten Jahren mindestens einen gravierenden Sicherheitsvorfall. Meist handelte es sich dabei um Attacken mittels Ransomware, Website-Hacking oder DDos-Attacken *(Quelle: IT-Sicherheitsumfrage 2020, eco – Verband der Internetwirtschaft e. V.)*

Aktuelle Vorfälle

- Microsoft Exchange Server
  - man geht von mindestens 26.000 verwundbaren Exchange Servern in Deutschland aus
  - auch viele kleine und mittlere Unternehmen sind betroffen


Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum
BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Mehrere Schwachstellen in MS Exchange

CSW-Nr. 2021-197772-1732, Version 1.7, 10.03.2021

IT-Bedrohungslage*: 4 / Rot

- Funke Mediengruppe: Ransomware, Dezember 2020
- Europäische Arzneimittelagentur (EMA): gezielter Angriff, Zugriff auf Dokumente im Zusammenhang mit dem Zulassungsantrag für den Corona-Impfstoff von Biontech und Pfizer
- Uniklink Düsseldorf: Ransomware, September 2020

Die häufigsten Bedrohungen

- Malware
- Ransomware (Erpressungstrojaner)
- DDoS (Distributed Denial of Service)
- Phishing, Identitätsmissbrauch/-diebstahl
- CEO Fraud (gefälschte Geschäfts-Mails)
- APT (Advanced Persistent Threat)
- Bot-Netze
- Website-Hacking

Quelle: Die Lage der IT-Sicherheit in Deutschland 2020, Bundesamt für Sicherheit in der Informationstechnik (BSI)

Cyber-Sicherheitslage für Deutschland 2020

Aktion und Reaktion

117,4 MIO.
neue Schadprogramm-Varianten

2019: 114 MIO.

durchschnittlich **322.000** neue Schadprogramm-Varianten pro Tag

in Spitzenwerten **470.000**

76 %
ist der Anteil unerwünschter **SPAM-MAILS** an allen in den Netzen des Bundes eingegangenen Mails

▶ 2019: 69 % ◀

24,3 MIO.
Patientendatensätze
waren Schätzungen zufolge international frei im Internet zugänglich

täglich bis zu **20.000**
BOT-INFEKTIONEN
deutscher Systeme

419
KRITIS-Meldungen

▶ 2019: 252
▶ 2018: 145

52.000 WEBSEITEN
wurden wegen enthaltener Schadprogramme durch die Webfilter der Regierungsnetze gesperrt

35.000
Mails mit Schadprogrammen
wurden durchschnittlich pro Monat in deutschen Regierungsnetzen abgefangen

109.000
Abonnenten Bürger-CERT

▶ 2019: 105.000
▶ 2018: 100.000

rund **100**
Produkte und Standorte
hat das BSI im Bereich Common Criteria zertifiziert

mehr als **4.400**
Mitglieder der Allianz für Cyber-Sicherheit

▶ 2019: 3.700
▶ 2018: 2.700

rund **1.700**
registrierte **KRITIS-Anlagen**

knapp **7 MIO.**
Meldungen zu Schadprogramm-INFEKTIONEN
übermittelte das BSI an deutsche Netzbetreiber

Quelle: Die Lage der IT-Sicherheit in Deutschland 2020, Bundesamt für Sicherheit in der Informationstechnik (BSI)

Ziele von Cyber-Angriffen

Alle! Privatpersonen und Unternehmen jeder Größe.

- Gezielte, individuelle Angriffe
- „Massenhacks“, Ausnutzung von Gelegenheiten

- Unterschiedliche Akteure
  - z.B. Sicherheitsexperten, Exploit Programmierer, Script Kiddies, (Ex-)Mitarbeiter; alleine oder vernetzt / stark organisiert
- Unterschiedliche Motivation
  - Spaß / Nervenkitzel, Ansehen, wirtschaftliche, politische oder militärische Interessen, Rache

Verschärfte Gefährdungslage durch die COVID-19-Pandemie

- Digitalisierung / remote work ist das „new normal“
- Bei der Umsetzung ging Schnelligkeit und Funktionalität vor Sicherheit
- Nicht ausreichend Zeit oder Gelegenheit für entsprechende Schulungen der Mitarbeitenden
- Ausnutzung der Situation durch Social Engineering

Häufige Angriffspunkte

- Angreifer suchen immer den einfachsten Weg
  - Home Office
  - Eigene IT-Systeme / Infrastruktur
  - Cloud Systeme
  - Faktor Mensch

- Grundsicherheit hat sich verbessert
  - Betriebssysteme sind insgesamt sicherer geworden
  - Hauptangriffspunkt ist (veraltete) Anwendungssoftware

Mögliche Folgen

- Datenverlust
- Unerwünschte Verbreitung von Informationen
- Imageverlust / gestörtes Vertrauen
- Betriebsausfall
- Hohe Folgekosten
- Rechtliche Risiken
- Erpressbarkeit

Prävention

- Risiko und Folgen abschätzen
  - „Notfallmanagement"
    (englisch: Business Continuity Management)
- Dokumentation der eigenen IT-Landschaft
- Schulungen, Handlungsanweisungen für Mitarbeiter
- Digitale Ersthelfer ausbilden
- Identitätsmanagement: Rechteverwaltung, Rollen
- Cyber-Versicherung

Konkrete IT-Sicherheitsmaßnahmen

- Absicherung der Systeme (Updates!)
- Netzwerk-Segmentierung
- Sichere Passwörter
  - 2FA wo es möglich ist
- Verschlüsselung
- Backup
- Löschen

Systeme absichern

- Wartungsaufwand schon bei der Beschaffung / Einrichtung neuer System mit einkalkulieren.
- Alle Systeme und Geräte regelmäßig updaten!
  - Betriebssystem
  - Anwendungssoftware
  - Web-Anwendungen
- Ggf. separate Geräte für beruflich und privat
  - zumindest separate Nutzerkonten

Passwort-Sicherheit

- Wichtige Konten besonders absichern, z.B.
  - E-Mail
  - Cloud-Speicher
  - Unternehmenskritische Anwendungen
- Separates Passwort für jeden Account
- Zugangsdaten sicher und gut organisiert verwahren
- Wenn möglich, 2-Faktor-Authentifizierung (2FA) verwenden
- Separate Accounts für zusätzliche Nutzer einrichten, statt Passwörter weiter zu geben
  - Zugriffsrechte einschränken
- https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/sichere-passwoerter-so-gehts-11672

Daten sichern

- Kein Backup – kein Mitleid!
  - verschiedene Medien und Aufbewahrungsorte
  - Wiederherstellung testen!
- Verschlüsselung
  - Wichtige, unternehmenskritische Daten
  - Personenbezogene Daten
  - So können Daten nicht in die falschen Hände geraten
  - z.B. Boxcryptor (https://www.boxcryptor.com/de/) [Business-Lizenz bestellen *]
- Löschen
  - Insbesondere personenbezogene Daten, die nicht mehr benötigt werden

* WERBUNG
Affiliate-Link, d.h. wenn Sie über diesen Link einen Kauf tätigen, erhalte ich möglicherweise eine Provision. An dem Endpreis für Sie ändert sich dadurch nichts.

Risikofaktor Mensch

- Social Engineering und Phishing-Angriffe, meistens über E-Mail
- Sensibilisieren
- Grundregel:
  - Niemals auf Links klicken, sondern direkt auf die Webseite des Anbieters gehen und über den gewohnten Weg einloggen.
- Bei dubiosen Anhängen oder Aufforderungen, die per Mail, Social Media oder Messenger zugesendet werden
  - Beim Absender persönlich rückversichern.

Beispiele für Phishing Mails

-------- Ursprüngliche Nachricht --------
Von: STRATO <info@tempel.asia>
Datum: 14.03.21 14:34 (GMT+01:00)
An: [redacted]
Betreff: Warnung: Ihre E-Mail wird bald blockiert

STRATO AG

sehr geehrter [redacted]

Ihr E-Mail-Konto läuft innerhalb von 24 Stunden ab, wenn Sie auf die Reaktivierungsschaltfläche unten klicken

Reaktivieren Sie Ihre E-Mail jetzt

Link-Adresse:
https://bit.ly/3liEq9o#MAILADRESSE

Sincerely,
Your STRATO team

Sehr geehrte Dame, sehr geehrter Herr,

Dies ist eine Benachrichtigung, um Sie darüber zu informieren, dass Ihr Domänenname angehalten wurde.
einzelheiten der aussetzung sind unten:

Domänennamen:
[redacted]

Grund für die aussetzung:
Unser abrechnungssystem hat festgestellt, dass Ihr Domainname abgelaufen ist, und nicht verlängert, obwohl
unsere vorherige erhöhung.

Sie sind eingeladen, das Verlängerungsformular für Ihre
Dienstleistungen nach den anweisungen und Schritten auf dem folgenden Link:

https://zahlung.strato.de

Wenn Sie sich nicht niederlassen, wird Ihr Domänenname in wenigen Stunden angehalten.

Zögern Sie nicht, unseren Kundenservice im Falle eines Problems oder für andere
Frage: support@strato.de

Strato ag
Pascalstraße 10
10587 Berlin

Von Mir <[redacted]@communibit.com> ☆ | Antworten | Weiterleiten | Archivieren | Junk | Löschen
Betreff **Mailbox Max Size Warning for account support@communibit.com** 10.03.2021,
An Mich <[redacted]@communibit.com> ☆

Email account quota configuration settings for [redacted]@communibit.com.

Mailbox Size Warning for account [redacted]@communibit.com
Some of your messages could not be sent.

The following users have exceeded their individual quota:
[redacted]@communibit.com
Go to your account to fix this issue.

Username:	[redacted]@communibit.com
Password:	Use the email account password.
Incoming Server:	IMAP Port: 993 POP3 Port: 995
Outgoing Server:	SMTP Port: 465

Go to your account

A .mobileconfig file for use with iOS for iPhone/iPad/iPod and MacOS® Mail.app® for Mountain Lion (10.8+) is attached to this message.

is notice is the result of a request made by a computer with the IP address [redacted]@communibit.com through the mail" service on the server.
e remote computer's location appears to be: Your Location.
e remote computer's IP address is assigned to your provider.
e system generated this notice on Friday, November 13, 2020 at 5:08:19 PM UTC.

his is an automated message, don't reply, your message will go nowhere.

Bei / Nach einem Vorfall

- Ausbreitung schnellstmöglich stoppen
- Systeme bereinigen
  - Nur 100%ig sichere Systeme wieder hochfahren
- Ursachen ermitteln und abstellen, damit es nicht wieder passiert!
- Beweise sichern
- Datenpannen melden
- Rechtliche Risiken
  - Datenschutz-Verstoß, Verstoß gegen sonstige gesetzliche Anforderungen (z.B. Meldepflicht, GoBD)
  - Verletzung vertraglicher Anforderungen gegenüber Kunden / Geschäftspartnern

Wo gibt es Unterstützung?

- Allianz für Cybersicherheit (z.B. IT-Notfallplan)
  - https://www.allianz-fuer-cybersicherheit.de
- IHK #gemeinsamdigital (Veranstaltungen)
  - https://www.dihk.de/de/themen-und-positionen/wirtschaft-digital/gemeinsamdigital
- IHK Downloads zum Thema Daten- und Informationssicherheit
  - https://www.ihk.de/daten-und-informationssicherheit
- Transferstelle für IT-Sicherheit im Mittelstand (Aktionsplan)
  - https://www.tisim.de
- Kompetenzzentrum digitales Handwerk (Routenplaner Cyber-Sicherheit für Handwerksbetriebe)
  - https://www.handwerkdigital.de

Ausblick

- Angreifer suchen und finden immer wieder neue Methoden
- Die Angriffsfläche wird immer größer
- Kosten durch Cyberkriminalität steigen

Fazit

- Wissen diffundiert auf vielen Wegen über Köpfe hinweg…
- Wissensvorsprung nicht mehr als alleinigen Wettbewerbsvorteil ansehen, stattdessen
  - Umsetzungsgeschwindigkeit, Marktzugang, Servicequalität
- **Gelebte IT-Sicherheitskultur**
  - nicht erst reagieren, wenn es zu spät ist!
- Interne **Ressourcen aufbauen** und/oder gute externe Partner suchen
  - Verfügbarkeit für zuverlässiges und schnelles Eingreifen sicherstellen

Ihre Internetagentur aus Wesel am Niederrhein

www.communibit.com