IT Security – GFAD Best Practice Leitfaden

Sehr geehrte Kunden,

wir möchten Sie darin unterstützen Ihr Unternehmen vor Datenverlust und Cyber-Angriffen zu schützen. Daher haben wir unseren Security Best Practice-Leitfaden inhaltlich und auch in Bezug auf das Format überarbeitet. Die hier beschriebenen Maßnahmen stellen den derzeit in der Branche - z.B. durch das BSI - anerkannten Standard dar (Stand 12.2021). Wir möchten Ihnen daher ans Herz legen, sich mit der Thematik auseinanderzusetzen. Wenn Sie Fragen oder Handlungsbedarf haben, gehen Sie auf Ihren GFAD-Ansprechpartner zu!

User

Strikte Passwort-Policy

Für die Windows-Accounts der User sind strikte Vorgaben für ausreichend komplexe Passwörter notwendig

Keine lokalen Administratorkonten

Lokale Administrationsrechte auf PCs sind beliebt - sie sind jedoch ein großes Sicherheitsrisiko

Regelmäßige User-Sensibilisierung

User sind regelmäßig durch sog. Awareness-Kampagnen für verdächtige Mails und Ähnliches zu sensibilisieren

Sinnvolle Berechtigungssystematik

Auf sensible Daten darf nicht jeder Mitarbeiter zugreifen - eine durchdachte Berechtigungs-Systematik ist daher ein „Must Have“

Zwei-Faktor-Authentifizierung

Remote-Zugänge wie z.B. der Microsoft365-Browser-Login oder VPN-Einwahlen müssen mit einem zweiten Faktor geschützt sein

Clients

Moderner Endpoint-Schutz

Moderne Anti-Malware, die auch gegen Verschlüsselungs-Trojaner schützt, gehört zum Standard

Festplattenverschlüsselung

Die Festplattenverschlüsselung schützt vor Datenverlust, wenn das Notebook gestohlen bzw. die Festplatte ausgebaut wird

Auf den Ernstfall vorbereiten!

Notfallplan

In Ihrem Bezirk fällt für 36 Stunden der Strom aus! Oder: ein Cyber-Angriff legt alles lahm. Haben Sie hierfür einen Notfallplan?

Testweise Backup-Rücksicherung

Backups zu haben ist gut. Um Überraschungen zu vermeiden, sollte die Rücksicherung regelmäßig getestet werden

Jährliche Simulation Stromausfall

Regelmäßige Tests stellen sicher, dass die USV funktioniert und alle System geordnet herunterfahren werden

Regelmäßige Überprüfungen!

IT Infrastrukturen unterliegen permanentem Wandel und die Angriffsszenarien werden immer raffinierter. Was gestern noch eine sinnvolle Konfiguration war, muss heute nicht mehr so sein oder ist sogar gefährlich.

Gerade bei langlebigen Themen (z.B. bei der Netzwerkstruktur) stellt sich die Frage nach dem richtigen Zeitpunkt der Weiterentwicklung. Da es diesen häufig gar nicht gibt, lautet die Antwort: Dann, wenn nach einer Überprüfung Handlungsbedarf festgestellt wird.

Daher: Spätestens alle drei Jahre sollte eine Infrastruktur durchgecheckt werden. Sprechen Sie uns an!

Angriffe Oktober bis Mitte Dezember 2021, Deutschland (Auswahl!)

MediaMarktSaturn
Hellmann Worldwide Logistics
Institut für Medizinische Informatik Statistik und Epidemiologie Leipzig
Eberspächer
medatixx GmbH
Talis Group
FTI GROUP
Stadtreinigung Leipzig
Stadtverwaltung Sassnitz
Technische Hochschule (TH) Nürnberg
Stadtwerke Pirna
Krankenhaus Braunschweig

Zentrale IT

Hardware im Support
Falls z.B. das Motherboard defekt ist, sollte die Reparatur durch den Hersteller in angemessener Zeit gewährleistet sein

Backup
Geschäftsrelevante Daten werden idealerweise nach dem Generationenprinzip gesichert und der Backupvorgang überprüft

Moderne Firewall
Eine Firewall ist ein Muss - nicht nur für klassische Funktionen, sondern z.B. auch für Webfilter und Ähnliches

USV für zentrale Systeme
Die unterbrechungsfreie Stromversorgung (USV) stellt bei Stromausfällen das geordnete Herunterfahren von Servern sicher

Backups außer Haus
Um auch gegen Elementarschäden gewappnet zu sein, lagert die zweite Backup-Stufe außer Haus bzw. online

Mail-Security
Ein- und ausgehende Mails werden sicherheitshalber auf Schadsoftware geprüft

Betriebssysteme im Support
Nicht mehr supportete Betriebssysteme sind ein eklatantes Sicherheitsrisiko, da es keine Security-Updates mehr gibt

Server-Monitoring
Die Überwachung von Servern ermöglicht das proaktive Handeln, um drohende Gefahren oder Ausfälle zu verhindern

Anti-Malware auf Servern
Auch Server - nicht nur PCs - müssen gegen Malware geschützt sein

Patch-Management
Ungepatchte Betriebssysteme sind ein Sicherheitsrisiko, daher gilt z.B. bei Microsoft Servern das monatliche Patchen als Standard

---

Neben diesem Standard gibt es weitere Maßnahmen, die wir ebenfalls empfehlen, aber noch nicht als absolutes Muss ansehen. Die Notwendigkeit der jeweiligen Maßnahme wird sinnvollerweise vor dem Hintergrund der Kunden-Situation und -Anforderungen diskutiert und bewertet:

Verschlüsselung
(z.B. Mailverschlüsselung)

Redundante Firewall-Appliances
… für höchste Verfügbarkeit

Redundante Server
… sorgen für Ausfallsicherheit

Client-Management
Für Überblick und bessere Steuerung

Mobile Device Management
Gewinnt an Bedeutung

XDR: Extended Detection & Response
Schutz, der über Anti-Malware hinausgeht

Nachrichten / Pressemitteilungen gehackter Unternehmen

„Am gestrigen Donnerstag drangen Hacker in die Systemwelt der FTI GROUP ein, sodass die Gruppe kurzzeitig weder buchbar noch erreichbar war."

„TALIS has on December 6th been impacted by a cyber security incident. As a part of managing the situation, some network services across our operations are suspended."

„Kriminelle haben die IT-System der Stadtwerke Pirna angegriffen […] Bei dringenden Angelegenheiten melden Sie sich telefonisch unter der kostenfreien Telefonnummer 0800 589 14 03."

„Hacker legen IT-Systeme des Autozulieferers Eberspächer lahm. Der Auspuffhersteller spricht von einem organisierten Angriff. Auch die Telefonverbindungen sind gekappt."

Kontakt
Telefon: 030 / 269 111 999
Mail: its-sales@gfad.de

Ihre Ansprechpartner (Sales Consulting):

Jaroslaw Andrzejewski
Thomas Gendreitzig
Robin Beck

Über die GFAD

Die GFAD IT und Service GmbH entstand ursprünglich als Abteilung der 1979 gegründeten GFAD Gruppe.

Die IT Infrastruktur-Tochter agiert jedoch seit langem als IT Systemhaus auch eigenständig am Markt. Zu unseren Kunden gehören mehrere hundert mittelständische Unternehmen in der Größenordnung 5 – 100 User.