IT-Sicherheit im Hotel

PEAKNET

„IT-Sicherheit muss weh tun und wenn es nicht weh tut, ist es nicht sicher.“

ABOUT US

PEAKNET

PEAKNET EDV Dienstleistungs GmbH ist IT-Infrastruktur Anbieter mit mehr als 30 Jahren Erfahrung im Hotel & Gastro Bereich, seit rund 10 Jahren mit Schwerpunkt auf gehärtete IT-Umgebungen und Netzwerksicherheit. Alex Kaiser ist Eigentümer & GF und leitet den Bereich Netzwerksicherheit.

Alex Kaiser

GF PEAKNET

Ein kurzer Überblick

Beispielhafter Ablauf einer Cyberattacke

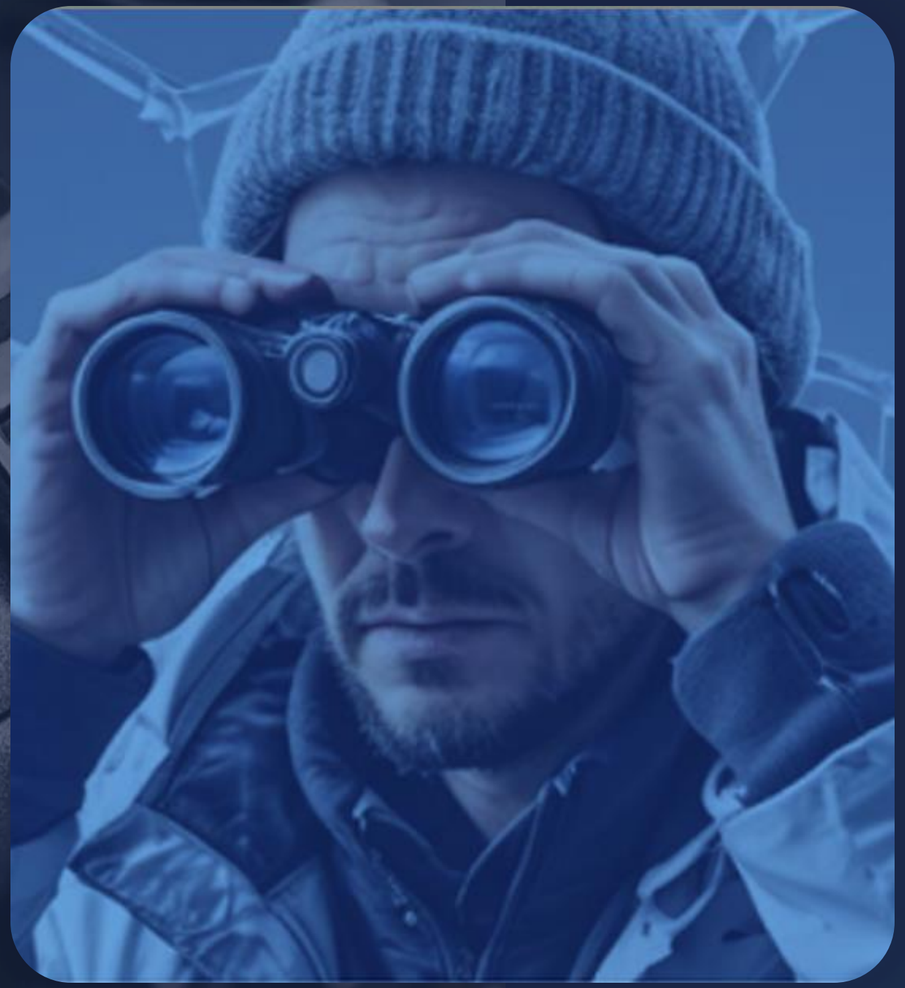
“Must haves” in der IT Security

Schritte zu einer sicheren IT

Spezialthemen

Die Phasen einer Cyberattacke

Aufklären, Eindringen, Umsehen, Eskalieren, Abschluss



Was bietet mein Ziel?

Suche nach öffentlich einsehbarern Informationen

Finanzdaten, Mitarbeiter und deren Funktionen, Webseiten und genutzte Clouddienste, IP Adressen, Informationen im Darknet

Analyse der internen und öffentlichen Kommunikation

Aufbau einer vertrauten Mailkommunikation, Studie der Corporate Identity, Erkennen interner Abläufe und Prozesse, Durchführung von Phishing-Angriffen

Scannen von Schwachstellen

Veraltete Firewallsysteme, offene Zugänge zu Diensten im Hotel, 0815 Passwörter/Passwortlisten

Den Fuß in die Türe bekommen

Ausnutzung von Schwachstellen

Exploit gegen veraltete Systeme, Zero-day Angriff, Schadsoftware via Email

Zugriff über erbeutete Zugangsdaten

Username/Password aus Phishing Angriffen, schwache Passwörter aus Passwortlisten, Passwortwiederverwendung zB aus dem Darknet

Gezieltes Festsetzen auf internen Systemen

Installation von Schadsoftware zur Fernsteuerung (Comand & Control Client/Server)

Was gibt es noch?

Scannen des internen Netzes

Auffinden weiterer verwundbarer Systeme, Verwendung gezielter Angriffssoftware um zusätzliche Geräte unter Kontrolle zu bringen

Weitere Passworte abgreifen

Installation von Keyboardloggern um “höherwertige” Zugangsdaten zu erbeuten

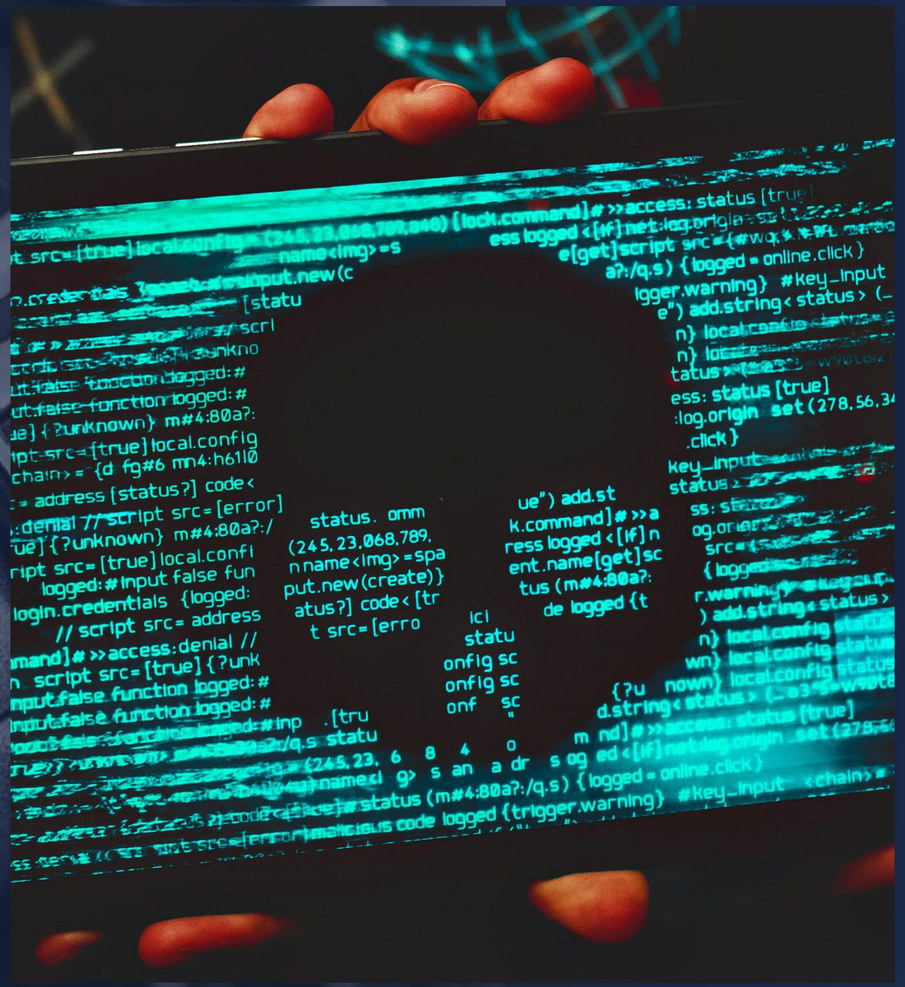
Feststellen von vorhandenen Sicherheitssystemen und Backups

Welche Sicherheitssysteme sind in Verwendung, wo liegen die Backups?

Admin, what else?

Eskalieren der Privilegien

Der Angreifer versucht auf allen, für seinen Angriff relevanten Systemen, Administrationsrechte zu bekommen.



Vollzug...

Backups löschen/verschlüsseln

Der Angreifer wird alle Backups, auf welche er Zugriff erlangt hat, löschen. Zumeist verbleibt ein Backup-Satz in verschlüsselter Form erhalten, um dafür Lösegeld zu erpressen.

Daten stehlen und danach löschen

Der Angreifer wird relevante Daten (Gästedaten, Kreditkartendaten, Verträge etc.) abgreifen, um in weiterer Folge mit der Veröffentlichung zu drohen. Final werden alle Daten gelöscht oder verschlüsselt.

Schritte zu einer sicheren IT

Quickcheck, Audit, Zertifizierung

Choose your plan

Quick-Check

Bestandsaufnahme, Risikoanalyse und erste Sicherungsmaßnahmen mit ihrem vertrauten IT-Partner und/oder einem externen IT-Sicherheitsspezialisten.

Get started

- Bestandsaufnahme und Risikoanalyse
- Umsetzung der “Must haves”
- Konzept für langfristige Absicherung

Audit

Umfangreicher Check mit externen IT-Sicherheitsspezialisten basierend auf anerkannten IT-Standards. Abschließende Durchführung eines Penetration-Tests.

Get started

- Umsetzung weiterer Maßnahmen
- IT-Standards zB BSI IT-Grundschutz
- Whitebox Penetration Test

Zertifizierung

Durchführung einer Zertifizierung nach einem IT-Sicherheitsstandard.

Get started

- ISO 27001
- DIN 66398
- Ergänzend ISAE 3402 (Typ II)

Welche Systeme habe ich im Haus?

Wissenschaftlicher Ansatz

- BSI Standard 200-2, IT-Grundschutz-Methodik, Basis-Absicherung

Praktischer Ansatz

- IT-System aufspüren (Netzwerkscans)
- In Anwendungen zusammenfassen (PMS, HKLS, etc)
- Nutzung bzw. Zuständigkeiten klären (Wer arbeitet damit?)
- Beschreibung von Konfiguration, Zustand, Wartung …
- Dokumentationen sichten bzw beschaffen
- Liegen Schwachstellen vor (Schwachstellen-Scans)

Wie ist das Backup aufgebaut?

Physischer Aufbau

- Wo stehen meine Backupsysteme?
- Welche Medien kommen zum Einsatz, und wo befinden sich diese?
- Wie viele Backupsätze gibt es?

Operativer Aufbau

- Wie oft wird was gesichert?
- Wer kontrolliert Backupprotokolle?
- Wer übernimmt die Fehlerbehebung?
- Werden Restoretests durchgeführt?

Zutritt und Zugriff

Rechte & Rollen erheben

- Welche Rollen gibt es im Unternehmen?
- Wie erfolgt deren Abbildung in den Rechtesystemen der Anwendungen?
- Wer teilt Rollen zu, wie oft wird kontrolliert?

Physische Sicherheit klären

- Wer hat Zutritt zu IT-Räumen?
- Können Zutritte protokolliert werden?
- Gibt es Videoüberwachung in den IT-Räumen?

Sechs Fragen zu jeder Anwendung

- Wie kritisch ist die Anwendung für das Unternehmen?
- Sind alle zugehörigen Komponenten aktuell und unter Wartung?
- Gibt es bekannte Schwachstellen?
- Ist sichergestellt, dass nur berechtigte Personen zugreifen düfen (minimal rights Prinzip)?
- Existiert ein sicheres Backup?
- Gibt es einen Notfallplan bei Ausfall?

Die ”must haves” in der IT Security

Schulung, MFA, Firewall, EDR, Backup, AD-Härtung, Netzwerksegmentierung

Mitarbeiter-schulung

Geschulte Mitarbeiter sind die erste Verteidigungslinie

- Erkennen von verdächtigen Emails und Webseiten (Phishing)
- Keine Verwendung fremder USB Geräte (Sticks)
- Ein Gast hat am Hotel-PC nichts verloren

Der richtige Umgang mit Passwörtern

- Keine Wiederverwendung von Passwörtern
- Sicheres Abspeichern in Password-Safes
- Keine Passwort.xls files!
- Vorgabe einer Mindestlänge (15, besser 20 Zeichen)
- zB “Bogart$schaut2augen”, “bertl!schwimmt1Geld”

Mehrfaktor-authentifizierung

Verwendung von MFA, wo immer die Möglichkeit besteht

- Office 365
- Webshops & Einkaufsportale
- Buchungsportale
- Cloud-PMS

Hardwaretoken bevorzugen

Wenn die Wahlmöglichkeit besteht, sind Hardware Token gegenüber One-Time-Passworten (OTP) bzw SMS-Token zu bevorzugen.

Die Zukunft liegt in “Passkeys”.

Eine Firewall, die ihren Namen verdient!

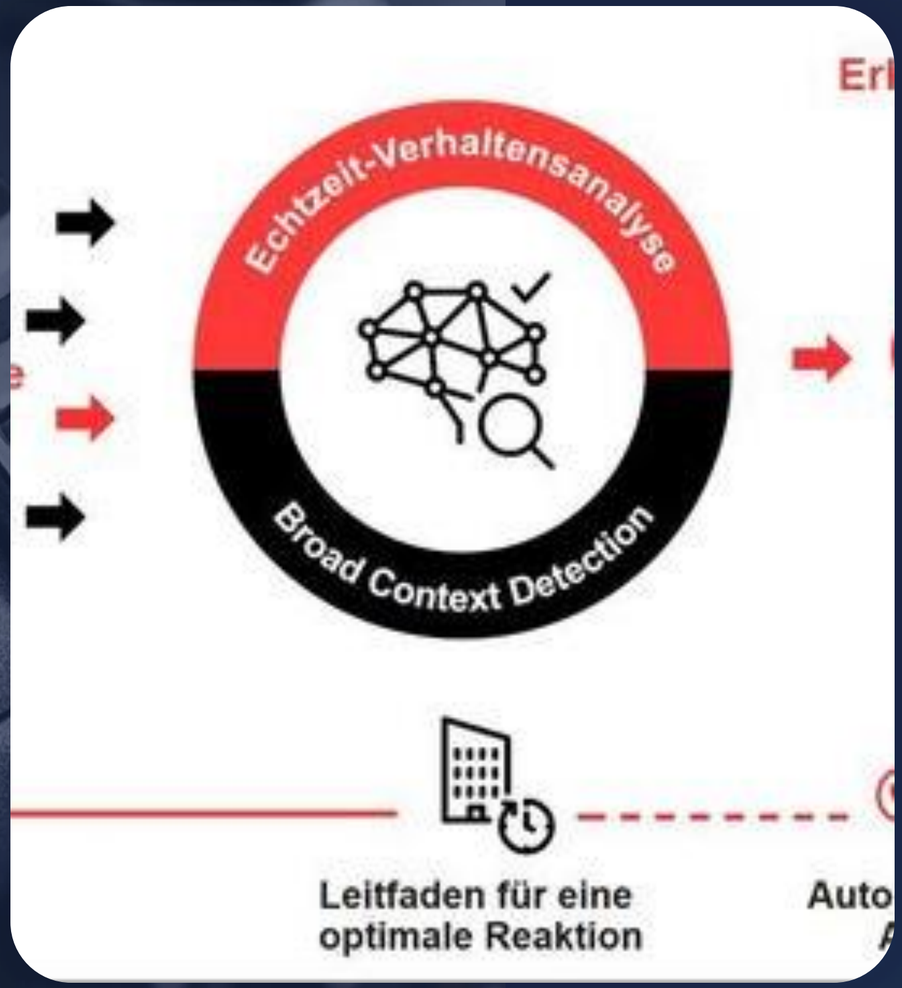
Eine gut konfigurierte Firewall schützt von innen

- Grundregel: Zero-Trust, was nicht bekannt ist, wird geblockt.
- Einsatz von Web- & DNS-Filtern (URL Filter)
- Verwendung von Geo-Blocks und IP-Sperrlisten

Zugriffe von extern reduzieren oder eliminieren

- Grundregel: Kein Zugriff von extern ohne VPN (E-Technik, HKLS, Videokameras …)
- Wo externe Zugriffe erforderlich sind, ist auf eine sichere Authentifizierung zu achten.

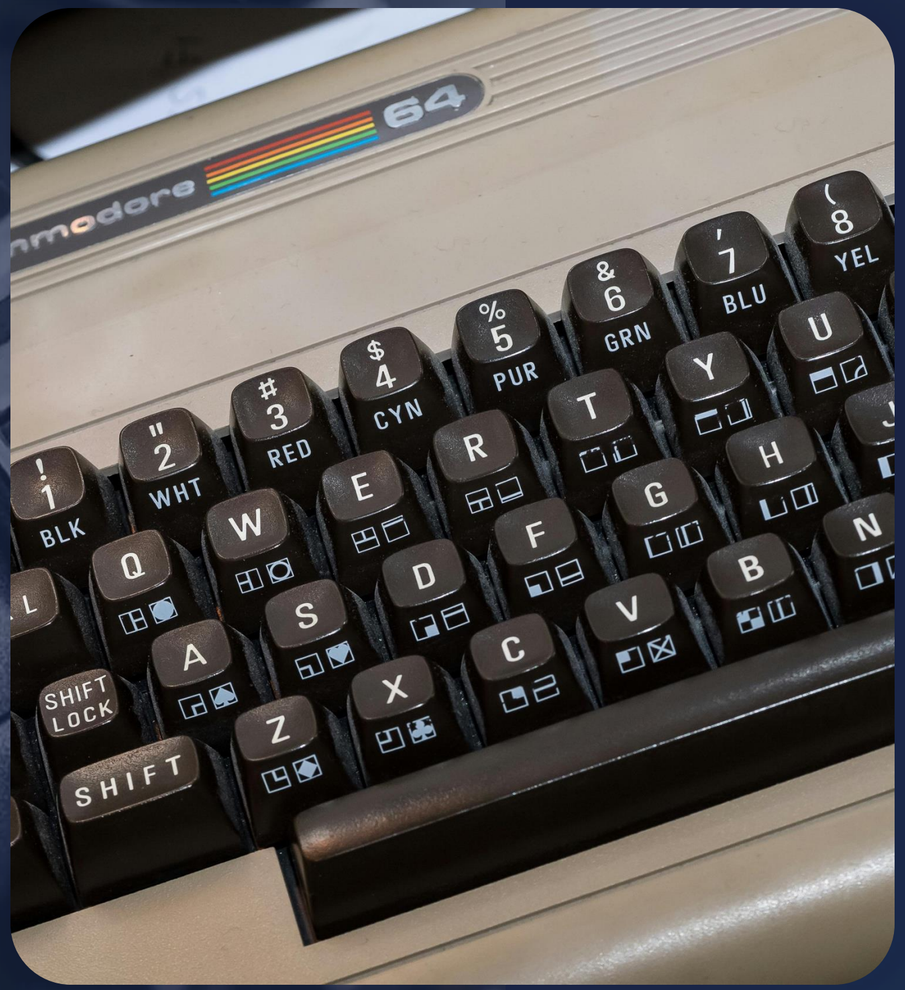
Firewall-Härtung ist ein dauernder Prozess



Endpoint Detection and Response

Klassischer Virenscanner und mehr

- Erkennt nicht nur Schadsoftware, sondern analysiert das Userverhalten und agiert bei ungewöhnlichen Vorgängen.
- Insbesondere bei Fehlverhalten des Users bieten EDR Lösungen einen guten Schutz.
- Gute Erkennung in Phase 3 eines Angriff: “Umsehen”
- Im Falle eines geglückten Angriffs bieten EDR Systeme umfangreiche Analysemöglichkeiten zur Aufklärung.



Legacy-Systeme loswerden

Legacy Systeme bieten Angriffsfläche

- Keine Wartung durch den Hersteller
- Keine Sicherheitspatches
- Hohes Risiko für Ausnutzung von Schwachstellen

Was bleibt, wird eingesperrt

- Wenn keine Netzwerkverbindung erforderlich ist, vom Netzwerk trennen
- Einsperren in eigenes Netzwerk, siehe Netzwerksegmentierung

Immutable- und Cloud Backup

Ein gutes Backup folgt der 3-2-1 Regel

- Mindestens 3 Instanzen Backups
- Davon mindestens 2 auf verschiedenen Medien
- Davon mindestens 1 “offsite”

Immutable Backup

- Gehärtetes Backupsystem mit nativem Schutz vor Manipulation
- Korrekte Konfiguration unbedingt erfoderlich

Cloud Backup

- Manipulationssicheres Backup zu einem Rechenzentrum
- zB Wasabi S3 Cloudspeicher

Sicherheit durch Netzwerk-Segmentierung

Jedem Gewerk seine “Farbe”

- Gewachsene Netzwerkstrukturen werfen sehr oft alle Anwendungen in einen ”Topf”
- 1. Schritt: E-Technik, HKLS, Poolsteuerungen, Videokameras etc. müssen in getrennte Netze
- 2. Schritt: PCs, Drucker, Backups und Server aufteilen
- 3. Schritt: Server werden nach ihren Funktionen getrennt.

Kommunikation untereinander nur über Firewalls

- Leistungsstarke Firewalls erforderlich
- Unbedingt redundante Firewallcluster verwenden

Spezialthemen

Cloud, Cyberversicherung

Kann die Cloud ihre Sicherheit erhöhen?

Die Nutzung der Cloud ist eine Verlagerung der Verantwortung

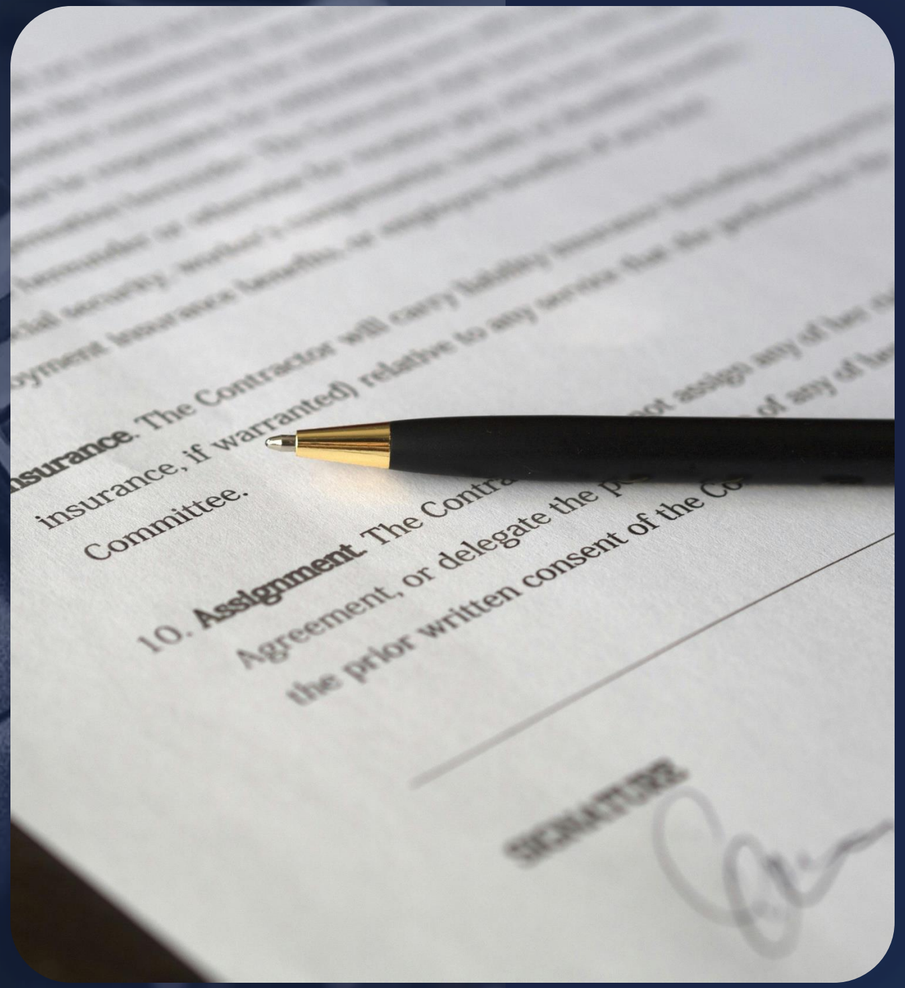
- Prüfen Sie die Reputation des Cloudpartners
- Verlangen Sie mehrmonatige Teststellungen

Erspart nicht die interne IT Sicherheit

- Nicht alles kann in die Cloud verlagert werden
- Eine Basisinfrastrruktur im Hotel bleibt erhalten und muss geschützt werden.

Cloud ist selten günstiger

- Cloud ist immer Subscription basierend – dh, laufende Kosten
- Dynamische Clouddienste müssen kostenseitig streng kontrolliert werden.



Benötige ich eine Cyber-versicherung?

Cyberversicherung ersetzt keine IT-Sicherheitsmaßnahmen

- Viele Versicherer bestehen auf Maßnahmen
- Ausbezahlte Versicherungsleistungen decken selten alle Aufwände

Achtung!

- Fragebögen zum Sicherheitszustand sind sehr sorgfältig und überlegt zu beantworten (Fallen)
- Prüfen Sie genau die Versicherungsleistungen

GLOSSAR

CEO-Fraud	Mit gefälschten Emails unter der Vorgabe von der Geschäftsführung des Unternehmens zu stammen, werden Mitarbeiter, zB der Buchhaltung, dazu gedrängt, Überweisungen an den Angreifer zu tätigen.
Command & Control	Systeme im Internet, welche vom Angreifer genutzt werden, um Geräte mit Schadsoftware fernzusteuern
Darknet	Teil des Internets, welches vom offiziellen Internet abgeschirmt wird und primär dem Datenaustausch krimineller Vereinigungen dient. Unter anderem erfolgt dort der Handel mit gestohlenen Daten.
Exploit	Ausnützen einer bekannten Schwachstelle eines Systems durch gezieltes Senden von Schadcode, um sich am System festzusetzen bzw Daten auslesen zu können. Beispielsweise im Internet erreichbare Server oder Firewalls können somit unter die Kontrolle des Angreifers gebracht werden.
Legacy-Systeme	Bezeichnung für veraltete IT-Systeme ohne Herstellersupport
Phishing	Ist von „Password-Fishing“ hergeleitet und stellt den Versuch dar, fremde Zugangsdaten zu stehlen. Vielfach angewendet in Form von gefälschten, identisch nachgebauten Websites, welche zur Eingabe von Benutzerdaten auffordern.
Whitebox Penetration Test	Dem Tester werden umfangreiche Informationen zum IT-System übergeben. Üblicherweise erhält er als Ausgangspunkt für seinen Test einen PC mit Userrechten. Ein Whitebox-Test reduziert die Kosten und bringt mehr Erkenntnisse über die innere Sicherheit der IT.
Zero-day	Bezeichnung für eine neue Schwachstelle, welche bisher noch gänzlich unbekannt war, bzw. vom Hersteller des Systems noch keine Behebungsmöglichkeiten (Patch) bereitgestellt wurden.

IT-Sicherheit im Hotel

Fragerunde