16.2 Malware, Ransomware und Schadsoftware im Detail

Malware ist ein Sammelbegriff für Schadsoftware.

Malware kann Systeme beschädigen, Daten ausspähen, Zugänge stehlen, Dateien verschlüsseln, Systeme fernsteuern oder Dienste stören.

Typische Malware-Arten:

- Virus
- Wurm
- Trojaner
- Ransomware
- Spyware
- Keylogger
- Rootkit
- Botnet-Client
- Cryptominer
- Adware
- Backdoor

Merksatz:

Malware ist Software mit schädlicher oder unerwünschter Funktion.

Warum Malware gefährlich ist

Malware kann verschiedene Schutzziele verletzen.

Vertraulichkeit:

Daten werden ausgespäht.
Passwörter werden gestohlen.
interne Informationen fließen ab.

Integrität:

Dateien werden verändert.
Systeme werden manipuliert.
Logs werden gelöscht.

Verfügbarkeit:

Systeme werden verschlüsselt.
Dienste fallen aus.
Dateien sind nicht mehr nutzbar.

Merksatz:

Malware kann Vertraulichkeit,
Integrität
und Verfügbarkeit gleichzeitig angreifen.

Typische Infektionswege

Malware gelangt häufig auf Systeme durch:

E-Mail-Anhänge
Phishing-Links
manipulierte Webseiten
unsichere Downloads
gecrackte Software
infizierte USB-Sticks
ungepatchte Schwachstellen
kompromittierte Updates
unsichere Makros
Remote-Zugänge
gestohlene Zugangsdaten
Supply-Chain-Angriffe

Merksatz:

Malware kommt oft über Menschen,
Schwachstellen

```
oder unsichere Softwarequellen ins System.
```

Virus

Ein Virus ist Schadsoftware, die sich an Dateien oder Programme anhängt.

Er wird meist aktiv, wenn die infizierte Datei ausgeführt wird.

Typische Merkmale:

```
braucht oft eine Wirtsdatei
verbreitet sich durch Weitergabe infizierter Dateien
kann Dateien verändern oder beschädigen
kann weitere Schadfunktionen nachladen
```

Merksatz:

```
Ein Virus hängt sich an Dateien oder Programme.
```

Wurm

Ein Wurm ist Schadsoftware, die sich selbstständig verbreiten kann.

Er nutzt häufig:

```
Netzwerkschwachstellen
unsichere Dienste
offene Ports
ungepatchte Systeme
schwache Zugangsdaten
```

Gefahr:

```
sehr schnelle Ausbreitung im Netzwerk
```

Merksatz:

```
Ein Wurm verbreitet sich selbstständig über Systeme oder Netzwerke.
```

Virus und Wurm vergleichen

Merkmal	Virus	Wurm
Verbreitung	meist über infizierte Datei	selbstständig über Netzwerk
braucht Wirtsdatei	häufig ja	nicht zwingend
Tempo	oft langsamer	oft schnell
typisches Risiko	Dateiinfektion	Massenausbreitung

Merksatz:

```
Virus braucht oft Hilfe.
Wurm verbreitet sich selbst.
```

Trojaner

Ein Trojaner tarnt sich als nützliches oder harmloses Programm.

Beispiele:

```
angeblicher Installer
gefälschtes Update
gecrackte Software
scheinbares Tool
manipuliertes Dokument
vermeintlicher Codec
```

Mögliche Schadfunktionen:

```
Zugangsdaten stehlen
Backdoor öffnen
weitere Malware nachladen
System fernsteuerbar machen
Daten ausspähen
```

Merksatz:

```
Ein Trojaner täuscht Nützlichkeit vor,
enthält aber Schadfunktionen.
```

Backdoor

Eine Backdoor ist ein versteckter Zugang zu einem System.

Angreifer nutzen Backdoors, um später erneut Zugriff zu bekommen.

Beispiele:

```
versteckter Benutzer
geöffneter Port
manipulierte Systemdatei
geheimer Fernzugriff
Schadsoftware mit Steuerkanal
```

Merksatz:

```
Backdoor = versteckter Hintereingang.
```

Ransomware

Ransomware ist Schadsoftware, die Daten verschlüsselt oder Systeme sperrt und anschließend Lösegeld fordert.

Typische Folgen:

```
Dateien nicht mehr nutzbar
Server nicht verfügbar
Produktionsausfall
Datenabfluss
Erpressung
hohe Wiederherstellungskosten
Vertrauensverlust
```

Merksatz:

Ransomware greift besonders die Verfügbarkeit an
und oft zusätzlich die Vertraulichkeit.

Ransomware-Ablauf vereinfacht

Ein typischer Ablauf:

1. Erstzugriff über Phishing,
   Schwachstelle
   oder Zugangsdaten.

2. Angreifer verschafft sich weitere Rechte.

3. Angreifer bewegt sich im Netzwerk.

4. Backups werden gesucht oder gelöscht.

5. Daten werden kopiert.

6. Systeme und Dateien werden verschlüsselt.

7. Lösegeldforderung erscheint.

Merksatz:

Ransomware ist oft kein einzelner Moment,
sondern eine Angriffskette.

Double Extortion

Double Extortion bedeutet:

Angreifer verschlüsseln Daten

und

drohen zusätzlich mit Veröffentlichung gestohlener Daten.

Dadurch wird nicht nur Verfügbarkeit, sondern auch Vertraulichkeit angegriffen.

Merksatz:

> Double Extortion kombiniert Verschlüsselung und Datenabfluss.

Schutz vor Ransomware

Wichtige Schutzmaßnahmen:

> regelmäßige Backups
> Immutable Backups
> Offline-Backups
> Restore-Tests
> Patchmanagement
> EDR
> MFA
> Least Privilege
> Netzwerksegmentierung
> Makros einschränken
> keine lokalen Adminrechte
> E-Mail-Schutz
> Monitoring
> schnelle Isolation infizierter Systeme

Merksatz:

> Gegen Ransomware helfen vor allem Backups,
> Rechtebegrenzung,
> Segmentierung
> und schnelle Reaktion.

Warum Backups gegen Ransomware wichtig sind

Wenn Daten verschlüsselt wurden, ist Wiederherstellung oft der wichtigste Weg zurück.

Aber Backups helfen nur, wenn sie:

vorhanden sind
aktuell genug sind
nicht mitverschlüsselt wurden
nicht gelöscht wurden
wiederherstellbar sind
regelmäßig getestet wurden
getrennt geschützt sind

Merksatz:

Backup ist nur dann Schutz,
wenn Restore funktioniert.

Immutable Backup bei Ransomware

Immutable Backup bedeutet:

Backup kann für eine festgelegte Zeit nicht verändert oder gelöscht werden.

Vorteile:

Schutz vor Angreifern mit Adminzugang
Schutz vor versehentlicher Löschung
Schutz vor Ransomware
bessere Wiederherstellungschance

Merksatz:

Immutable Backups erschweren das Löschen oder Manipulieren von Sicherungen.

Spyware

Spyware ist Schadsoftware, die Informationen heimlich sammelt.

Mögliche Ziele:

Passwörter
Browserdaten
E-Mails
Tastatureingaben
Bildschirmaufnahmen
Dateien
Nutzungsverhalten
Zugangstokens

Merksatz:

Spyware spioniert Daten und Verhalten aus.

Keylogger

Ein Keylogger zeichnet Tastatureingaben auf.

Ziele:

Passwörter
Zugangsdaten
Kreditkartendaten
Nachrichten
interne Informationen

Keylogger können sein:

Software
Hardware
Bestandteil anderer Malware

Merksatz:

Keylogger stehlen Eingaben direkt an der Tastatur.

Rootkit

Ein Rootkit versteckt Schadsoftware oder Angreiferaktivitäten tief im System.

Ziele:

```
Erkennung verhindern
Kontrolle behalten
Prozesse verstecken
Dateien verstecken
Logs manipulieren
Sicherheitssoftware umgehen
```

Rootkits sind besonders kritisch, weil sie schwer zu erkennen und zu entfernen sein können.

Merksatz:

```
Rootkits verstecken Angriffe tief im System.
```

Botnet-Client

Ein Botnet-Client ist ein infiziertes System, das von Angreifern ferngesteuert wird.

Viele solcher Systeme bilden ein Botnet.

Nutzung:

```
DDoS-Angriffe
Spamversand
Credential Stuffing
Malware-Verteilung
Cryptomining
Proxy-Missbrauch
```

Merksatz:

```
Botnet = viele fremdgesteuerte infizierte Systeme.
```

Cryptominer

Ein Cryptominer missbraucht Rechenleistung, um Kryptowährung zu berechnen.

Folgen:

```
hohe CPU- oder GPU-Last
hohe Stromkosten
langsame Systeme
Überhitzung
Cloud-Kostenanstieg
verringerte Systemleistung
```

Merksatz:

```
Cryptominer stiehlt Rechenleistung.
```

Adware

Adware zeigt unerwünschte Werbung an oder verändert Browser- und Systemeinstellungen.

Mögliche Folgen:

```
störende Werbung
Browserumleitungen
Tracking
Installation weiterer unerwünschter Software
reduzierte Benutzerfreundlichkeit
```

Merksatz:

```
Adware ist oft weniger zerstörerisch,
aber trotzdem unerwünscht und riskant.
```

Malware-Erkennung

Malware kann erkannt werden durch:

```
Antivirus
EDR
ungewöhnliche Prozesse
ungewöhnliche Netzwerkverbindungen
hohe CPU-Last
```

```
geänderte Dateien
verdächtige Autostarts
Warnungen im SIEM
auffällige DNS-Anfragen
ungewöhnliche Loginversuche
bekannte Signaturen
Verhaltensanalyse
```

Merksatz:

```
Malware-Erkennung kombiniert Signaturen,
Verhalten
und Monitoring.
```

Signaturbasierte Erkennung

Signaturbasierte Erkennung nutzt bekannte Muster.

Beispiel:

```
bekannte Schadsoftware-Datei
bekannte Hashwerte
bekannte Codebestandteile
bekannte Angriffsmuster
```

Vorteil:

```
gut gegen bekannte Malware
```

Nachteil:

```
schwächer gegen neue oder veränderte Malware
```

Merksatz:

```
Signaturen erkennen Bekanntes.
```

Verhaltensbasierte Erkennung

Verhaltensbasierte Erkennung achtet auf verdächtiges Verhalten.

Beispiele:

```
viele Dateien werden schnell verändert
Prozess startet ungewöhnliche Befehle
Programm öffnet unbekannte Netzwerkverbindung
Benutzerkonto greift plötzlich auf viele Systeme zu
Skript lädt ausführbare Datei nach
```

Vorteil:

```
kann auch neue oder veränderte Angriffe erkennen
```

Merksatz:

```
Verhaltenserkennung erkennt Auffälligkeiten,
auch wenn die Datei noch unbekannt ist.
```

Antivirus

Antivirus-Software erkennt und blockiert bekannte Schadsoftware.

Typische Funktionen:

```
Dateiprüfung
Echtzeitschutz
Signaturprüfung
Quarantäne
Scans
Erkennung bekannter Malware
```

Grenze:

```
Antivirus allein reicht nicht als Sicherheitskonzept.
```

Merksatz:

```
Antivirus ist wichtig,
aber nur eine Schutzschicht.
```

EDR

EDR steht für:

```
Endpoint Detection and Response
```

EDR überwacht Endgeräte stärker als klassischer Antivirus.

Typische Funktionen:

```
Prozessüberwachung
Verhaltensanalyse
Angriffserkennung
Isolation eines Endgeräts
Untersuchung von Vorfällen
zentrale Auswertung
Reaktionsmaßnahmen
```

Merksatz:

```
EDR hilft,
Angriffe auf Endgeräten zu erkennen und darauf zu reagieren.
```

Quarantäne

Quarantäne bedeutet:

```
Eine verdächtige oder schädliche Datei wird isoliert.
```

Ziel:

```
Datei kann nicht weiter ausgeführt werden.
Schaden wird begrenzt.
Datei kann später untersucht werden.
```

Merksatz:

```
Quarantäne isoliert verdächtige Dateien.
```

Isolation eines Endgeräts

Wenn ein Gerät infiziert ist, sollte es schnell isoliert werden.

Isolation bedeutet:

```
vom Netzwerk trennen
WLAN deaktivieren
Netzwerkkabel ziehen
EDR-Isolation nutzen
VPN trennen
Zugriff auf Server sperren
```

Wichtig:

```
Nicht unüberlegt ausschalten,
wenn forensische Analyse benötigt wird.
```

Merksatz:

```
Infizierte Systeme schnell vom Netz trennen,
aber Vorgehen dokumentieren.
```

Malware und Rechte

Malware hat oft nur die Rechte des Benutzers, unter dem sie ausgeführt wird.

Wenn Benutzer lokale Adminrechte haben, kann Malware mehr Schaden anrichten.

Schutz:

```
keine lokalen Adminrechte für Alltag
Least Privilege
getrennte Admin-Konten
```

Applikationskontrolle
Rechteprüfung

Merksatz:

Weniger Benutzerrechte bedeuten weniger Malware-Schaden.

Malware und Netzwerksegmentierung

Wenn ein System infiziert ist, darf sich Malware nicht frei im Netzwerk bewegen können.

Segmentierung hilft durch Trennung von:

Clientnetz
Servernetz
Managementnetz
Backupnetz
Produktionsnetz
Gastnetz
IoT-Netz

Merksatz:

Segmentierung begrenzt Ausbreitung.

Laterale Bewegung

Laterale Bewegung bedeutet:

Angreifer oder Malware bewegen sich nach dem ersten Zugriff weiter im Netzwerk.

Beispiele:

Zugriff von Client auf Dateiserver
Zugriff auf weitere Clients
Auslesen von Zugangsdaten
Angriff auf Domain Controller

Zugriff auf Backups
Angriff auf Managementsysteme

Merksatz:

Laterale Bewegung ist Ausbreitung nach dem Erstzugriff.

Schutz vor lateraler Bewegung

Maßnahmen:

Netzwerksegmentierung
Firewall zwischen Netzbereichen
Least Privilege
keine lokalen Adminrechte
getrennte Admin-Konten
MFA
EDR
Monitoring
sichere Passworthygiene
Zugriff auf Adminfreigaben begrenzen

Merksatz:

Nach dem ersten kompromittierten System darf nicht das ganze Netz offen sein.

Makros als Risiko

Office-Makros können nützlich sein, werden aber oft für Malware missbraucht.

Risiken:

Makro lädt Schadsoftware nach
Makro führt Befehle aus
Makro startet Skripte
Benutzer aktiviert Inhalt aus Täuschung

Schutz:

```
Makros aus dem Internet blockieren
nur signierte Makros erlauben
Benutzer schulen
E-Mail-Anhänge prüfen
Office-Härtung nutzen
```

Merksatz:

```
Makros nur erlauben,
wenn sie wirklich benötigt und vertrauenswürdig sind.
```

Skripte als Risiko

Skripte können für Administration nützlich sein, aber auch von Angreifern missbraucht werden.

Beispiele:

```
PowerShell
Bash
JavaScript
VBScript
Python
Batch-Dateien
```

Risiken:

```
Malware nachladen
Dateien verschlüsseln
Systeme ausspähen
Befehle automatisieren
Sicherheitssoftware umgehen
```

Merksatz:

```
Skripte sind mächtig und brauchen Kontrolle.
```

Application Control

Application Control bedeutet:

Es wird gesteuert,
welche Programme ausgeführt werden dürfen.

Beispiele:

nur freigegebene Anwendungen
keine Ausführung aus Download-Ordner
keine unbekannten Skripte
keine unsignierten Programme
Blockierung bekannter Risikopfade

Merksatz:

Application Control verhindert,
dass beliebige Programme starten.

Allowlisting

Allowlisting bedeutet:

Nur ausdrücklich erlaubte Programme oder Aktionen sind zugelassen.

Vorteil:

sehr restriktiv
reduziert unbekannte Schadsoftware

Nachteil:

höherer Verwaltungsaufwand
kann Benutzer einschränken
muss gut gepflegt werden

Merksatz:

Allowlisting erlaubt nur Bekanntes und Freigegebenes.

Blocklisting

Blocklisting bedeutet:

Bekannte schädliche Programme oder Aktionen werden verboten.

Vorteil:

einfacher einzuführen

Nachteil:

neue oder unbekannte Malware kann durchkommen

Merksatz:

Blocklisting verbietet Bekanntes,
erlaubt aber Unbekanntes oft weiterhin.

Patchmanagement gegen Malware

Viele Malware-Angriffe nutzen bekannte Sicherheitslücken.

Patchmanagement schützt, indem Updates geplant und eingespielt werden.

Betroffen sind:

Betriebssysteme
Browser
Office-Programme
Serverdienste
VPN-Gateways
Firewalls
Anwendungen
Firmware

Container-Images

Merksatz:

Ungepatchte Systeme sind leichte Ziele.

E-Mail-Schutz gegen Malware

Viele Malware-Angriffe beginnen per E-Mail.

Schutzmaßnahmen:

Spamfilter
Malware-Scanner
Linkprüfung
Anhangprüfung
Blockierung gefährlicher Dateitypen
Makroregeln
Absenderprüfung
SPF,
DKIM
und DMARC
Benutzerschulung

Merksatz:

E-Mail-Schutz ist eine wichtige erste Verteidigungslinie.

Download-Schutz

Downloads können Malware enthalten.

Schutzmaßnahmen:

nur vertrauenswürdige Quellen
Signaturen prüfen
Hashwerte prüfen
keine gecrackte Software

Browser-Schutz
EDR
Rechtebegrenzung
Softwareverteilung zentral steuern

Merksatz:

Software nur aus vertrauenswürdigen Quellen installieren.

USB-Geräte als Risiko

USB-Geräte können Malware verbreiten oder Daten stehlen.

Risiken:

infizierter USB-Stick
manipuliertes Eingabegerät
Datenabfluss
automatische Ausführung
unbekannte Geräte

Schutz:

USB-Richtlinien
Gerätekontrolle
AutoRun deaktivieren
Schulung
nur freigegebene Geräte
Verschlüsselung
DLP je nach Umgebung

Merksatz:

Unbekannte USB-Geräte nicht vertrauen.

DLP

DLP steht für:

```
Data Loss Prevention
```

DLP soll verhindern, dass sensible Daten unkontrolliert abfließen.

Beispiele:

```
Blockieren von Uploads
Warnung bei sensiblen Daten in E-Mail
Schutz vor Kopieren auf USB
Kontrolle von Cloud-Freigaben
Erkennung von Kreditkartennummern oder Personaldaten
```

Merksatz:

```
DLP schützt vor unerwünschtem Datenabfluss.
```

Malware und Cloud

Auch Cloud-Umgebungen können von Malware betroffen sein.

Beispiele:

```
infizierte VM
kompromittierter Container
Malware in Storage
gestohlene API-Schlüssel
Cryptomining in Cloud-Instanzen
Ransomware in synchronisiertem Cloud-Speicher
```

Schutz:

```
IAM
MFA
EDR für Cloud-VMs
sichere Images
Container-Scanning
Security Groups
Logging
```

Kostenalarme

Merksatz:

Cloud schützt nicht automatisch vor Malware.

Malware und Container

Container können Schadsoftware enthalten, wenn Images unsicher sind.

Risiken:

manipuliertes Image
veraltete Bibliothek
unsichere Registry
eingebettete Secrets
Container läuft mit zu vielen Rechten
unsichere Runtime-Konfiguration

Schutz:

Images scannen
nur vertrauenswürdige Registries
minimale Images
keine Secrets im Image
keine unnötigen Rechte
regelmäßige Updates

Merksatz:

Container-Images müssen wie Software geprüft werden.

Malware und Backups

Backups können ebenfalls Malware enthalten.

Problem:

Wenn ein Backup bereits infizierte Dateien enthält,
kann Malware nach Restore wieder aktiv werden.

Wichtig:

Backup-Zeitpunkt wählen
Infektionszeitpunkt bestimmen
Restore testen
Systeme vor Wiederanbindung prüfen
Backups nicht ungeprüft zurückspielen

Merksatz:

Restore nach Malware braucht sorgfältige Prüfung.

Erste Maßnahmen bei Malware-Verdacht

Sinnvolle Schritte:

1. Ruhe bewahren.
2. System vom Netzwerk isolieren.
3. Zeitpunkt und Symptome dokumentieren.
4. IT-Sicherheit oder Verantwortliche informieren.
5. Keine Beweise unnötig löschen.
6. Logs sichern.
7. Betroffene Konten prüfen.
8. Ausbreitung prüfen.
9. Ursache analysieren.
10. Bereinigung oder Neuaufbau planen.
11. Wiederherstellung testen.
12. Maßnahmen verbessern.

Merksatz:

Bei Malware zählt schnelle Eindämmung und saubere Dokumentation.

Neuinstallation statt Bereinigung

Bei schwerer Kompromittierung ist Neuinstallation oft sicherer als reine Bereinigung.

Gründe:

```
Rootkits schwer erkennbar
Backdoors möglich
Systemdateien manipuliert
Rechte verändert
Logs gelöscht
Vertrauen ins System verloren
```

Merksatz:

```
Ein kompromittiertes System ist oft nicht mehr vollständig vertrauenswürdig.
```

Typische Malware-Symptome

Mögliche Anzeichen:

```
System wird sehr langsam
unbekannte Prozesse
hohe CPU-Last
viele Netzwerkverbindungen
Dateien verschwinden
Dateien werden verschlüsselt
Antivirus meldet Fund
ungewöhnliche Popups
Browser leitet um
Benutzerkonto verhält sich auffällig
neue Autostart-Einträge
unerklärliche Cloud-Kosten
```

Merksatz:

```
Malware zeigt sich oft durch ungewöhnliches Verhalten.
```

Typische Schutzmaßnahmen gegen Malware

Wichtige Maßnahmen:

```
Patchmanagement
Antivirus
EDR
E-Mail-Schutz
MFA
Least Privilege
keine lokalen Adminrechte
Makro-Schutz
Application Control
Netzwerksegmentierung
regelmäßige Backups
Immutable Backups
Restore-Tests
Monitoring
Logging
Benutzerschulung
Incident Response
```

Merksatz:

```
Malware-Schutz braucht mehrere Schutzschichten.
```

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

```
- Was ist Malware?
- Was ist der Unterschied zwischen Virus und Wurm?
- Was ist ein Trojaner?
- Was ist Ransomware?
- Warum ist Ransomware besonders gefährlich?
- Was bedeutet Double Extortion?
- Wie schützt man sich vor Ransomware?
- Warum sind Backups gegen Ransomware wichtig?
- Was ist Spyware?
- Was ist ein Keylogger?
```

- Was ist ein Rootkit?
- Was ist ein Botnet?
- Was ist ein Cryptominer?
- Was ist der Unterschied zwischen Antivirus und EDR?
- Was bedeutet Quarantäne?
- Warum ist Netzwerksegmentierung gegen Malware wichtig?
- Was ist laterale Bewegung?
- Warum sind Makros ein Risiko?
- Was ist Application Control?
- Was ist DLP?
- Warum reicht Antivirus allein nicht aus?

Typische Prüfungsfallen

Malware ist ein Oberbegriff.

Virus und Wurm nicht verwechseln.

Wurm verbreitet sich selbstständig.

Trojaner tarnt sich als nützlich.

Ransomware betrifft Verfügbarkeit
und oft Vertraulichkeit.

Double Extortion bedeutet Verschlüsselung plus Datenabfluss.

Backup verhindert Ransomware nicht,
ermöglicht aber Wiederherstellung.

Replikation ersetzt kein Backup.

Backup muss vor Manipulation geschützt sein.

Antivirus allein reicht nicht.

EDR erkennt und reagiert umfassender.

Quarantäne bedeutet Isolation einer Datei.

Infiziertes Gerät schnell isolieren.

Lokale Adminrechte erhöhen Schaden.

Segmentierung begrenzt Ausbreitung.

Laterale Bewegung ist Bewegung im Netzwerk nach Erstzugriff.

Makros und Skripte sind häufige Angriffsmittel.

Allowlisting ist strenger als Blocklisting.

Cloud ist nicht automatisch frei von Malware.

Container-Images müssen geprüft werden.

Restore nach Malware braucht Vorsicht.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Malware	Schadsoftware
Virus	Schadsoftware mit Wirtsdatei
Wurm	selbstverbreitende Schadsoftware
Trojaner	getarnte Schadsoftware
Backdoor	versteckter Zugang
Ransomware	erpresserische Verschlüsselung oder Sperrung
Double Extortion	Verschlüsselung plus Datenabfluss
Spyware	Spionagesoftware
Keylogger	zeichnet Tastatureingaben auf
Rootkit	versteckt und verankert Schadsoftware
Botnet	Netzwerk fremdgesteuerter Systeme
Botnet-Client	infiziertes ferngesteuertes System
Cryptominer	missbraucht Rechenleistung
Adware	unerwünschte Werbesoftware

Begriff	Kurze Erklärung
Antivirus	Schutz gegen bekannte Schadsoftware
EDR	Endpoint Detection and Response
Quarantäne	Isolation verdächtiger Dateien
Isolation	Trennung eines Systems vom Netzwerk
laterale Bewegung	Ausbreitung im Netzwerk
Makro	automatisierte Funktion in Dokumenten
Application Control	Steuerung erlaubter Programme
Allowlisting	nur Erlaubtes zulassen
Blocklisting	Bekanntes verbieten
DLP	Data Loss Prevention
Restore	Wiederherstellung
Immutable Backup	unveränderliches Backup
Incident Response	Reaktion auf Sicherheitsvorfall

IHK-sichere Kurzformulierung

Malware ist ein Oberbegriff für Schadsoftware wie Viren, Würmer, Trojaner, Ransomware, Spyware, Keylogger, Rootkits, Botnet-Clients und Cryptominer. Ein Virus hängt sich häufig an Dateien oder Programme an, während sich ein Wurm selbstständig über Netzwerke verbreiten kann. Ein Trojaner tarnt sich als nützliches Programm, enthält aber Schadfunktionen. Ransomware verschlüsselt Daten oder sperrt Systeme und fordert Lösegeld. Schutzmaßnahmen gegen Malware sind Patchmanagement, Antivirus, EDR, MFA, Least Privilege, Netzwerksegmentierung, Makroschutz, Application Control, E-Mail-Schutz, Backups, Immutable Backups, Restore-Tests, Logging, Monitoring und Benutzerschulung.

Merksätze

Malware ist Schadsoftware.

Virus hängt sich an Dateien.

Wurm verbreitet sich selbstständig.

Trojaner täuscht Nützlichkeit vor.

Backdoor ist versteckter Zugang.

Ransomware verschlüsselt oder sperrt.

Double Extortion = Verschlüsselung plus Datenabfluss.

Spyware spioniert.

Keylogger stehlen Tastatureingaben.

Rootkits verstecken Angriffe.

Botnet besteht aus fremdgesteuerten Systemen.

Cryptominer stiehlt Rechenleistung.

Malware kann alle Schutzziele verletzen.

Infektionswege sind oft E-Mail,
Download,
Schwachstelle
oder Zugangsdaten.

Antivirus erkennt vor allem bekannte Malware.

EDR erkennt und reagiert tiefer.

Signaturen erkennen Bekanntes.

Verhaltenserkennung erkennt Auffälligkeiten.

Quarantäne isoliert verdächtige Dateien.

Infizierte Systeme schnell isolieren.

Weniger Rechte bedeuten weniger Schaden.

Segmentierung begrenzt Ausbreitung.

Laterale Bewegung verhindern.

Makros aus unsicheren Quellen blockieren.

Skripte kontrollieren.

Allowlisting ist strenger als Blocklisting.

Patchmanagement schließt bekannte Lücken.

E-Mail-Schutz ist wichtig.

USB-Geräte nicht blind vertrauen.

DLP schützt vor Datenabfluss.

Cloud braucht ebenfalls Malware-Schutz.

Container-Images prüfen.

Backups können infizierte Daten enthalten.

Restore nach Malware sorgfältig planen.

Neuaufbau kann sicherer sein als Bereinigung.

Malware-Schutz braucht mehrere Schichten.