Dallmeier

CYBERSECURITY BEI VIDEOSICHERHEITSSYSTEMEN

BEST PRACTICE GUIDE




MADE IN GERMANY

See more.

CYBERSECURITY BETRIFFT AUCH DIE VIDEOTECHNIK

Für wen ist dieses Dokument?

Dieser Best Practice Guide richtet sich in erster Linie an:

- Integratoren von Videosicherheitssystemen
- Netzwerkadministratoren
- IT-Sicherheitsverantwortliche
- Führungskräfte
- Entscheidungsträger

Cybersecurity als eine der größten Herausforderungen

Heutige Videosicherheitssysteme sind wie alle modernen vernetzten Geräte komplizierte Computersysteme. Daher können beispielsweise Hacker versuchen, die Kontrolle über die Systeme zu erlangen. Aber auch die Benutzer selbst können durch ihr Verhalten die Sicherheit des gesamten Netzwerks und Unternehmens gefährden. Dementsprechend gehört die Datensicherheit bzw. Cybersecurity mittlerweile zu einer der größten Herausforderungen bei der Planung, Realisierung und Erweiterung digitaler Netzwerkinfrastrukturen für moderne Videosicherheitssysteme.

Dallmeier setzt auf „Security by Design"

Video-IP-Produkte von Dallmeier werden daher mit einem besonderen Augenmerk auf den Faktor „Cybersecurity" entwickelt. Die Sicherheit digitaler Informationen bei deren Verarbeitung hat bei Dallmeier oberste Priorität. Jedes Produkt, egal ob Hardware oder Software, unterliegt dabei einem kontinuierlichen Verbesserungsprozess, um stets die neuesten technologischen Sicherheitsstandards zu erfüllen. Dallmeier Netzwerk-Produkte werden dazu regelmäßig internen und externen Penetrationstests unterzogen. Somit kann Dallmeier auf aktuelle Cyber-Bedrohungen schnell reagieren und einen optimalen Schutz vor den neuesten Angriffsszenarien sicherstellen.

Cybersecurity als Prozess verstehen

Doch erst ein konsistentes Netzwerk-Sicherheitskonzept und dessen Anwendung auf allen eingesetzten Geräten, Komponenten und Anwendungen ermöglicht, ein Videosicherheitssystem effektiv und erfolgreich gegen Cyber-Angriffe abzusichern.

NÜTZLICHE DOKUMENTE UND INFORMATIONEN

Der Best Practice Guide als hilfreicher Leitfaden

Der vorliegende Best Practice Guide gibt allgemeine Hinweise auf die wichtigsten Sicherheitsmaßnahmen für Videosicherheitssysteme sowie bewährte Praktiken zum effektiven Schutz von digitalen Netzwerkinfrastrukturen. Es kann helfen, kritische Schwachstellen im Netzwerk zu identifizieren, um es gegen Bedrohungen durch zielgerichtete Angriffe von außen oder innen wirksam zu schützen.

Dallmeier Produktdokumentationen

Dieser Best Practice Guide beschreibt die wichtigsten Maßnahmen zur Absicherung von digitalen Netzwerk- infrastrukturen nur allgemein. Detaillierte Informationen und Beschreibungen zu Dallmeier Produkten finden Sie in der jeweiligen Produktdokumentation auf www.dallmeier.com.

Dritthersteller Produktinformationen

Aktuelle Dokumentationen zu Produkten von Drittherstellern, wie Router, Switche, Firewalls, Virenschutz-Programme etc. finden Sie üblicherweise im Internet auf den entsprechenden Produktseiten des jeweiligen Herstellers.

Weitere Empfehlungen und Richtlinien

Informieren Sie sich zudem auch bei den jeweils staatlich anerkannten Stellen in Ihrem Land über die neuesten gesetzlichen Vorgaben, Richtlinien und Empfehlungen. In Deutschland beispielsweise beim Bundesamt für Sicherheit in der Informationstechnik (BSI) unter https://www.bsi.bund.de.


00:00:02.625

Inhalt

BEST PRACTICE AUF EINEN BLICK

Dieses Kapitel gibt einen ersten Überblick über das Thema Cybersecurity. Basierend auf den drei maßgeblichen IT-Sicherheitszielen **Vertraulichkeit**, **Integrität** und **Verfügbarkeit** wird die jeweilige Bedeutung für Videosicherheitssysteme aufgezeigt. Ergänzend verweisen wir auf die Funktionen des Datenschutz- und Datensicherheitsmoduls von Dallmeier und geben erste Best Practice Empfehlungen.

IT-Sicherheitsziel	Bedeutung für Videosicherheit
Vertraulichkeit Vertraulichkeit bezeichnet den Schutz vor unbefugter Preisgabe und Änderung von Informationen.	Geeignete Maßnahmen sollen sicherstellen, dass Daten des Videosicherheitssystems sicher, vertraulich und vor unberechtigter Kenntnisnahme geschützt sind.
Integrität Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen.	Geeignete Maßnahmen sollen sicherstellen, dass Daten und Funktionen des Videosicherheitssystems nicht versehentlich oder absichtlich manipuliert werden und somit echt, zurechenbar und vollständig sind.
Verfügbarkeit Die Verfügbarkeit von Diensten und Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.	Geeignete Maßnahmen sollen sicherstellen, dass Daten und Funktionen des Videosicherheitssystems zur Verfügung stehen und vor Fremdzugriffen geschützt sind.

BEST PRACTICE AUF EINEN BLICK

Detaillierte Informationen zu den Funktionen des Dallmeier Datenschutz- und Datensicherheitsmoduls erhalten Sie in der Broschüre: „Videosicherheit, Datenschutz und Datensicherheit“. Mehr dazu auf Seite 19.

Dallmeier Datenschutz- und Datensicherheitsmodul

- Benutzergruppen-Verwaltung
- Vier-Augen-Login-Prinzip
- Zeitlich begrenzter Zugriff “MaxView”

- Ende-zu-Ende-Verschlüsselung (Daten und Videostream)
- Security Gateway “ViProxy”
- Backdoor-Schutz
- Gerichtsverwertbare Aufzeichnungen (LGC-Zertifikat)

- Sicheres Netzwerk-Authentifizierungsverfahren (IEEE 802.1X)
- Schutz vor Hackerangriffen (Fail2Ban)
- Failover- und Redundanzmechanismen

Ausgewählte Best Practices

- Standard-Zugangskennungen ändern und stattdessen starke Passwörter verwenden (S. 12)
- Regelmäßige Software- und Firmware-Updates einspielen (S. 15)
- Deaktivierung nicht benötigter Benutzerkonten (S. 17)

- Netzwerk-Segmentierung durch: Separates Unternehmens- und Videonetzwerk, Einsatz von VLANs (S. 8)
- Unsichere Netzwerk-Ports sperren (bei Dallmeier Video-IP-Produkten schon ab Werk gesperrt) (S. 12)

- Zeitsynchronisierung sicherstellen und System-Logs aktivieren (S. 10)
- Deaktivierung nicht benötigter Dienste (S. 12)

TECHNISCHE MAßNAHMEN

Dieses Kapitel beschreibt die wichtigsten technischen Maßnahmen und Strategien zur Absicherung von digitalen Netzwerkinfrastrukturen. Zudem werden einige Lösungsansätze und Sicherheitsfunktionen vorgestellt, die in Dallmeier Geräten und Applikationen implementiert wurden.

Netzwerksegmentierung

Ein netzwerkbasiertes Videosicherheitssystem sollte immer in einem separaten Netzwerk betrieben werden. Damit wird zunächst ein ungewollter Datenfluss zwischen den Komponenten des Videosystems und Arbeitsstationen anderer Unternehmensbereiche verhindert. Entscheidend ist aber, dass die Anzahl der möglichen Angriffspunkte auf das Videonetzwerk erheblich reduziert wird.

Physische Trennung

Die sicherste Methode separate Netzwerke zu realisieren, ist eine physische Trennung der Netzwerksegmente. Dabei werden keine gemeinsam genutzten Switches eingesetzt, und jegliche kabelgebundene Verbindung zwischen den Segmenten wird unterbunden.

VLAN

Da die physische Netzwerk-Segmentierung mit einem erhöhten Kosten- und Verwaltungsaufwand verbunden ist, bietet sich die Nutzung eines eigenen virtuellen LAN (VLAN) für das Videonetzwerk an. VLANs erlauben die Definition mehrerer logisch getrennter Netzwerksegmente auf einer einheitlichen physischen Infrastruktur.

ViProxy

Wenn das Videosicherheitssystem in einem separaten Netzwerk betrieben wird, ist in manchen Fällen dennoch ein Zugriff auf die Live-Bilder und Aufzeichnungen aus dem Arbeitsnetzwerk erwünscht. Hier bietet sich die Nutzung der Funktion ViProxy an, die von allen Dallmeier Aufzeichnungssystemen unterstütz wird.

ViProxy erlaubt unter anderem die Nutzung der ersten Ethernet-Schnittstelle des Aufzeichnungssystems zur Anbindung an das Videosystem. Die zweite Ethernet-Schnittstelle wird für die Anbindung an das Arbeitsnetzwerk genutzt. Die Funktion ViProxy dient dabei als Security-Gateway / Proxy-Server und verhindert unberechtigten Zugriff auf das Videomaterial.

Netzwerkinfrastruktur

Managed Switches

In einem netzwerkbasierten Videosicherheitssystem sollten nur Managed Switches eingesetzt werden. Diese ermöglichen die Deaktivierung von nicht genutzten Netzwerkanschlüssen. Somit kann vermieden werden, dass nicht autorisierte Geräte über eine nicht genutzte LAN-Schnittstelle Zugriff auf das Netzwerk erhalten.

MAC-Adressfilterung

Managed Switches bieten in der Regel Funktionen zur MAC-Adressfilterung. Diese erlaubt es, nur eine bestimmte Liste von Geräten zu definieren, die mit dem Switch verbunden werden können. Andere am Switch angeschlossene Geräte werden ignoriert, auch wenn der Port zuvor von einem gültigen Gerät verwendet wurde.

DHCP

Dallmeier Kameras und Aufzeichnungssysteme unterstützen das Dynamic Host Configuration Protocol (DHCP). Dies ermöglicht die Zuordnung von Netzwerkeinstellungen (IP-Adresse, Subnet, Gateway) über einen zentralen DHCP-Server.

Wenn die Netzwerkeinstellungen über einen DHCP-Server und nicht direkt am Gerät konfigurieren werden, sollte immer statisches DHCP verwenden werden. In diesem Modus werden am DHCP-Server die IP-Adressen den entsprechenden MAC-Adressen manuell zugeordnet. Die vergebenen IP-Adressen können dann von keinem anderen Gerät, das nachträglich an das Netzwerk angeschlossen wird, verwendet werden.

TECHNISCHE MAßNAHMEN

Zeitserver

Das netzwerkbasierte Videosicherheitssystem sollte mit einem Zeitserver ausgestattet sein, an dem sich alle Geräte mittels Network Time Protocol (NTP) synchronisieren. Damit wird sichergestellt, dass auf allen Geräten die korrekte Zeit und das korrekte Datum eingestellt ist, um eine Auswertung von Protokolldateien bzw. Ereignisprotokollen zu ermöglichen.

SNMP-Überwachung

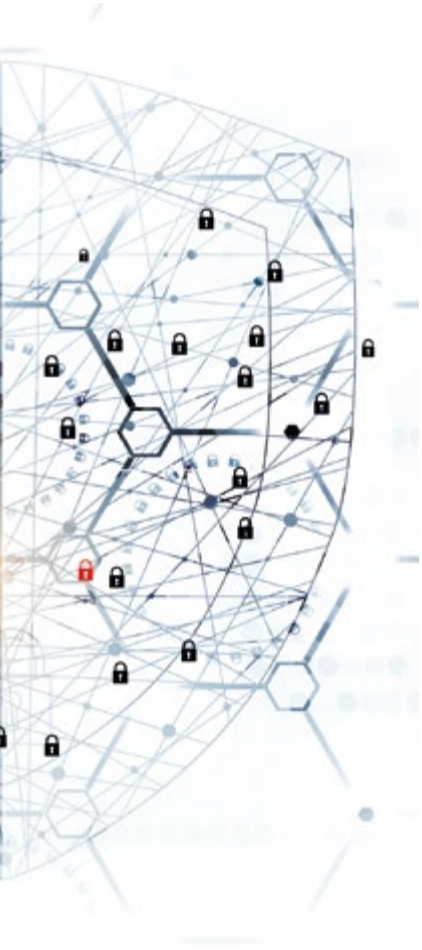
Das Simple Network Management Protocol (SNMP) erlaubt die Überwachung aller Geräte eines Netzwerks von einer zentralen Station aus und wird von allen Dallmeier Aufzeichnungssystemen und Kameras unterstützt. Hierbei muss beachtet werden, dass die Versionen 1 und 2 des SNMP-Protokolls fast keine Sicherheitsmechanismen bieten. Daher sollte immer nur SNMP v3 zur Überwachung der Geräte verwendet werden.

Wireless LAN

Auf WLAN-Verbindungen sollte in einem netzwerkbasierten Videosicherheitssystem aus Sicherheitsgründen grundsätzlich verzichtet werden. WLAN-Netzwerke bringen eine besonders hohe Gefahr von Man-in-the-Middle-Angriffen mit sich.

Mobiler Zugriff

Für den mobilen Zugriff auf Videodaten bietet Dallmeier die DMVC Server Software. Diese ermöglicht sowohl die Anzeige von Live-Bildern als auch die Wiedergabe von Aufzeichnungen auf mobilen Endgeräten mithilfe der entsprechenden Dallmeier App. Die DMVC App ist in den bekannten App-Stores für verschiedene mobile Betriebssysteme erhältlich.



Authentifizierung und Verschlüsselung

Netzwerkauthentifizierung

Ein netzwerkbasiertes Videosicherheitssystem sollte durch den Einsatz einer sicheren Authentifizierung nach dem Standard IEEE 802.1X abgesichert werden. Diese Netzwerkfunktion überprüft neu angeschlossene Geräte anhand von Zertifikaten (EAP-TLS) und unterbindet jegliche Netzwerkkommunikation im Fall einer fehlenden Berechtigung. Damit kann das Risiko eines Man-in-the-Middle-Angriffs nahezu ausgeschlossen werden.

Verschlüsselung

Der Einsatz einer End-to-End verschlüsselten Video- und Datenübertragung mit TLS 1.2/AES 256 Bit über DaVids und HTTPs bietet höchsten Schutz vor unberechtigtem Zugriff auch innerhalb eines netzwerkbasierten Videosicherheitssystems. Bei dieser Technik handeln die Netzwerkteilnehmer, beispielsweise eine Kamera und ein Aufzeichnungssystem, einen geheimen Schlüssel zur Kodierung der übertragen Daten aus. Da dieser nur den Endgeräten bekannt ist, kann ein Mitlesen der Video- und Datenübertragung durch andere Netzwerkteilnehmer verhindert werden.

Betriebssysteme von Kamera- und Aufzeichnungssystemen

Dallmeier Kamera- und Aufzeichnungssysteme sind mit einem in Hinblick auf die Systemsicherheit stark angepassten und abgeschotteten (hardened) Linux Betriebssystem ausgestattet. Dieses bietet keine Möglichkeit, ein fremdes Programm einzuschleusen oder auszuführen

TECHNISCHE MAßNAHMEN

Dienste und Ports

Im kompletten IT-System sollten alle nicht benötigten Dienste und Ports deaktiviert werden, um Angriffspunkte zu minimieren. Zudem sollten regelmäßig alle auf Servern und Client-PCs laufenden Dienste mithilfe eines Port-Scanning-Programms überprüft werden.
Auf Dallmeier Geräten sind ab Werk alle technisch unsicheren Ports wie beispielsweise für UPnP, Telnet oder FTP geschlossen.

Zugriffskontrolle

Im gesamten IT-System sollte Zugriff auf Geräte nur nach einer erfolgreichen Authentifizierung mit Benutzernamen und Passwort erfolgen dürfen, um einen wirksamen Schutz vor Daten-Manipulation sicherzustellen. Für das netzwerkbasierte Videosicherheitssystem sollten strengere Anforderungen beachtet werden.

Standardpasswörter

Die Kameras und Aufzeichnungssysteme eines Videosicherheitssystems werden werkseitig immer mit Standardpasswörtern für den unproblematischen Zugriff ausgeliefert. Diese sollten unbedingt bereits bei der ersten Inbetriebnahme durch neue und strenge Passwörter ersetzt werden.

Vier-Augen-Prinzip

Zur Vermeidung des unberechtigten Zugriffs auf Aufzeichnungen sollten Dallmeier Aufzeichnungssysteme durch das Vier-Augen-Login-Prinzip abgesichert werden. In diesem Fall ist der Zugriff nur mit einem zusätzlichen Passwort einer zweiten Person möglich.

TECHNISCHE MAßNAHMEN

Admin Account

Alle Geräte eines Videosicherheitssystems sollten mit einem vollberechtigten Admin Account für vollberechtigte Systemadministratoren ausgestattet werden. Für Techniker, die beispielsweise mit der Wartung der Geräte beauftragt sind, sollten immer gesonderte Benutzer Accounts mit beschränkten Rechten eingerichtet werden.

Client Software

Neben den Kameras und Aufzeichnungssystemen sollten auch die Auswertestationen eines Videosicherheitssystems durch strenge Passwörter abgesichert werden. Die Client-Software für die Auswertung von Live-Bildern und Aufzeichnungen sollte durch gesonderte Passwörter für die verschiedenen Benutzergruppen zusätzlich abgesichert werden.

Benutzergruppen

Die Berechtigungen für die verschiedenen Benutzergruppen sollten immer nach dem geforderten Datenschutz-Level festgelegt und nachweissicher dokumentiert werden. Diese kann bereits direkt an den Kameras, Aufzeichnungssystemen und der Client-Software erfolgen, oder optional mit einer zentralisierten Benutzerverwaltung über einen AD-Verzeichnisdienst mittels LDAP.

Fernkonfiguration

Dallmeier bietet die Software PService für die einfache und zentrale Inbetriebnahme und Verwaltung eines Videosicherheitssystems an. Nach der Inbetriebnahme und Konfiguration der einzelnen Geräte des Systems sollte die Option zur Fern-Konfiguration der IP-Adresse über PService aus Sicherheitsgründen immer deaktiviert werden.

TECHNISCHE MAßNAHMEN

Internetanbindung

Demilitarisierte Zone (DMZ)

Um Sicherheitsrisiken von außen zu minimieren, sollten Computer und Server mit sensiblen Daten nicht über das Internet direkt erreichbar sein. Dies gilt natürlich auch für Kameras, Aufzeichnungssysteme und Video-Management-Anwendungen.
Falls dennoch ein Zugriff von außen erforderlich ist, sollte eine sogenannte demilitarisierte Zone (DMZ) eingerichtet werden. Eine DMZ ist ein spezieller Netzwerkbereich, durch den das interne Netz (LAN) vom Internet (WAN) mithilfe von Firewalls abgeschottet wird. Für höchste Sicherheit sollte eine DMZ mit zwei Firewalls unterschiedlicher Hersteller realisiert werden, falls eine Schwachstelle in der Firewall eines Herstellers überwunden wird.

Firewalls

Für kleinere Netzwerke kann die Einrichtung einer demilitarisierten Zone (DMZ) einen unverhältnismäßig hohen Auswand darstellen. Als Schutz vor Einbruchsversuchen in das lokale Netz sollten zumindest spezielle Firewall-Rechner eingerichtet und mit restriktiven Firewall-Regeln konfiguriert werden. Der Einsatz von Firewalls bietet sich auch innerhalb von Unternehmen an, um Bereiche unterschiedlicher Sensitivität voneinander abzugrenzen.

Internet PC

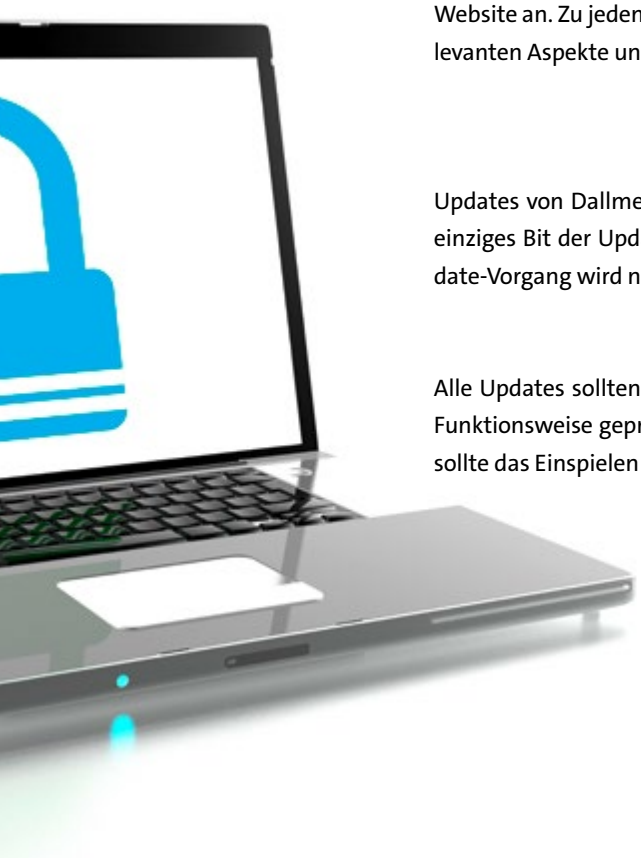
Um die Mehrkosten und den Administrationsaufwand für eine DMZ bei kleinen Unternehmen zu vermeiden, kann ein gesonderter PC, ohne Verbindung zum internen Netzwerk, für Recherchen im Internet genutzt werden. Heruntergeladene Dateien können dann zunächst lokal auf schädlichen Code geprüft werden und, gegebenenfalls per Datenträger in das interne Netz transferiert werden.

Virtual Private Network (VPN)

Für Heimarbeiter, die eine Verbindung ins Firmennetzwerk benötigen, sollte der Zugriff auf das interne Netz über ein Virtual Private Network (VPN) erfolgen. Dabei sollte das VPN-Protokoll durch eine Verschlüsselung ergänzt werden, die eine abhör- und manipulationssichere Kommunikation erlaubt und somit höchste Anforderungen an die Übertragungssicherheit erfüllt.

Patch Management

Alle Netzwerkkomponenten (Firewalls, Router, Switches etc.) des kompletten IT-System sollten insbesondere in Bezug auf Sicherheitspatches stets auf dem aktuellsten Software-Stand sein. Auch die Betriebssysteme von Servern und Client-PCs sollten unbedingt regelmäßig auf Sicherheitspatches geprüft und falls erforderlich entsprechend aktualisiert werden.



Dallmeier bietet Software-Updates für alle Kameras und Aufzeichnungssysteme auf der Dallmeier Website an. Zu jedem Update wird eine technische Mitteilung veröffentlicht, die über alle sicherheitsrelevanten Aspekte und Neuerungen informiert.

Updates von Dallmeier sind immer gegen Veränderungen durch Dritte abgesicherten. Sobald nur ein einziges Bit der Update-Datei modifiziert wurde, wird es nicht mehr als gültig akzeptiert und der Update-Vorgang wird nicht eingeleitet.

Alle Updates sollten zunächst ausgiebig in einer Testumgebung auf Kompatibilität und einwandfreie Funktionsweise geprüft werden, um den laufenden Betrieb des IT-Systems nicht zu gefährden. Zudem sollte das Einspielen von Updates stets sorgfältig geplant und dokumentiert werden.

ALLGEMEINE MAßNAHMEN

Dieses Kapitel beschreibt allgemeine Präventivmaßnahmen rund um das Thema Cybersecurity und gibt weitere Empfehlungen, die Sie unterstützen sollen, die Sicherheit von Daten und IT-Systemen in Ihrem Unternehmen zu erhöhen.

Grundlegendes

Unternehmensweites Sicherheitskonzept einführen

Führen Sie ein konsistentes unternehmensweites Sicherheitskonzept ein. Prüfen Sie die darin festgelegten Richtlinien und dessen Umsetzung mithilfe von genau definierten Checklisten.

Sicherheitsmaßnahmen dokumentieren

Dokumentieren Sie getroffene Sicherheitsmaßnahmen ausführlich und verständlich. Sicherheitsrelevante Aufgabenstellungen müssen auch dann gemeistert werden können, wenn der zuständige Systemadministrator oder IT-Sicherheitsexperte einmal nicht verfügbar sein sollte.

Schulungen und Weiterbildungen organisieren

Organisieren Sie regelmäßig Schulungen und Weiterbildungen für Fach- und Führungskräfte sowie für Mitarbeiter, um die Sensibilität für IT-Sicherheit und Datenschutz aufrechtzuerhalten und auf aktuelle Cyber-Bedrohungen vorbereitet zu sein.

Penetrationstests durchführen

Stellen Sie sicher, dass regelmäßig Penetrationstests sowohl intern als auch extern durchgeführt werden, um potentielle Schwachstellen Ihrer IT-Systeme möglichst schnell identifizieren und beheben zu können.

Mitarbeitern die Verwendung eigener Datenträger verweigern

Verweigern Sie Mitarbeitern das Verwenden eigener Datenträger, um einen möglichen Datendiebstahl zu vermeiden.

Zugriffsrechte

Nicht benötigte Benutzerkonten deaktivieren

Prüfen Sie, ob bei der Installation von Betriebssystemen auf Ihren Servern mehrere Benutzerkonten angelegt wurden, wie beispielsweise ein Gastkonto oder Hilfskonto zur Remote-Unterstützung. Deaktivieren Sie nicht benötigte Accounts, um die Sicherheit Ihrer Systeme zu erhöhen.

Mitarbeitern die eigenständige Installation von nicht geprüfter Software verweigern

Stellen Sie sicher, dass Mitarbeiter nicht eigenständig fremde Software auf Client-PCs installieren, um die Risiken von Angriffen auf Ihre IT-Systeme durch Computerviren oder Ransomware zu minimieren.

Systemlogs prüfen

Prüfen Sie regelmäßig die Ereignisprotokolle Ihrer Anwendungen Netzwerkkomponenten und Videosicherheitssysteme, um sicherheitsrelevante Vorkommnisse wie unberechtigte Zugriffsversuche schnell aufzuspüren.

Administrative Zugriffsrechte beschränken

Beschränken Sie die Anzahl von Systemadministratoren, die volle Zugriffsrechte auf Ihre IT-Systeme haben. Setzen Sie nur vertrauenswürdige, nicht korrumpierbare Personen in sicherheitsrelevanten Bereichen ein.

Passwörter für vertretungsberechtigte Systemadministratoren sicher hinterlegen

Bereits vor Abwesenheit eines vollständig privilegierten Systemadministrators müssen berechtigte Personen benannt sein, die dann in dessen Vertretung temporär den vollen Zugriff auf die entsprechenden IT-Systeme erhalten. Dazu ist es zwingend notwendig, die entsprechenden Passwörter sicher zu dokumentieren und zu hinterlegen (z. B. in einem geschlossenen Umschlag in einem Safe). Jeder Zugriff auf die hinterlegten Passwörter (Vier-Augen-Prinzip empfohlen) muss dokumentiert werden.

ALLGEMEINE MAßNAHMEN

Physischer Schutz

Kameras und Netzwerkgeräte an schwer zugänglichen Stellen montieren

Montieren Sie Kameras und andere Netzwerkkomponenten, wie etwa Router, nur an schwer zugänglichen Stellen, um Hardware-Manipulationen oder gar eine Zerstörung der Geräte zu vermeiden. Aufzeichnungssysteme sollten grundsätzlich in gegen unbefugten Zugriff abgesicherten Serverräumen aufgestellt werden.

Zutrittskontrollsysteme installieren

Installieren Sie Zutrittskontrollsysteme zu Netzwerkräumen und anderen sicherheitsrelevanten Bereichen, um ausschließlich berechtigten Personen Zugang zu sensitiven Daten und Systemen zu gewähren.

Daten- und Systemwiederherstellung

Datensicherung durchführen

Führen Sie regelmäßig Datensicherungen (Backups) durch und lagern Sie diese an einem sicheren und separaten Ort. Backups sollten in periodischen Abständen erfolgen, um sich wirksam vor Datenverlust zu schützen. Prüfen Sie Backups zudem stichprobenartig auf ihre Fehlerfreiheit und Wiederherstellbarkeit.

Systemabbilder erstellen

Erstellen Sie regelmäßig Systemabbilder (Images) für eine schnelle Wiederherstellung Ihrer IT-Systeme im Falle einer Infektion durch Schadprogramme (Malware) oder möglicher Festplattenschäden.

ANMERKUNGEN

Themen-Website „Cybersecurity“

Besuchen Sie unsere Themen-Webseite zu Videosicherheit und Cybersecurity. Dort finden Sie weitere hilfreiche Informationen kompakt an einer Stelle:

Rechtlicher Hinweis

Die Inhalte dieses Dokuments werden nur zu Informationszwecken bereitgestellt. Sie stellen keine erschöpfende Beratung hinsichtlich des Schutzes vor Cyberbedrohungen dar. Dallmeier garantiert nicht, dass seine Produkte gegen potenzielle Cyberangriffe immun sind. Zudem kann Ihr Videosicherheitssystem bzw. Netzwerk auch dann von einem Cyberangriff bedroht sein, wenn Sie die Inhalte dieses Dokuments umsetzen.

Dallmeier

Dedicated to quality. Driven by passion.

Dallmeier electronic GmbH & Co.KG
Bahnhofstr. 16
93047 Regensburg
Germany

Tel: +49 941 8700-0
Fax: +49 941 8700-180
info@dallmeier.com
www.dallmeier.com

MADE IN GERMANY

See more.