Sicherheitstechnik Kortus

Schließanlagen & elektronische Zutrittskontrollen

Erklärungsmaterial:
Die 3 Sicherheitsbegriffe im Kontext der NIS 2-Richtlinie

Zutrittskontrolle - Zugang - Zugriff

Sicherheitstechnik Kortus
Brauhof 3, 04626 Schmölln
www.schliessanlage-kaufen.de
info@schliessanlage-kaufen.de | Tel: 034491 82186

Fragen? Termin bei Herr Kortus buchen.

1. ZUTRITTSKONTROLLE

Definition

Zutrittskontrolle ist die physische Kontrolle darüber, wer einen bestimmten Raum oder Bereich betreten darf. Sie ist die erste Sicherheitsschicht und wirkt vor allen anderen Kontrollmechanismen.

Detaillierte Erklärung

Zutrittskontrolle bedeutet wörtlich: Kontrolle über den Zutritt - also den Eintritt in einen physischen Raum. Stellt euch einen Serverraum vor: Diese Tür ist die Zutrittskontrolle. Niemand kann hinein, ohne die richtige Berechtigung zu haben - sei es ein Schlüssel, eine Magnetkarte oder ein biometrisches System. Zutrittskontrolle ist immer physisch, immer greifbar, und sie ist die erste Verteidigungslinie. Wenn jemand hier abgewiesen wird, können alle dahinterliegenden IT-Systeme noch so sicher sein - es spielt keine Rolle, denn diese Person kommt erst gar nicht rein.

Praktische Beispiele

- Schlüssel im Schloss (mechanisch)
- Magnetkarte an der Schleuse
- PIN-Code an der Eingangstür
- Biometrische Erkennung (Fingerabdruck, Iris)
- Wachperson, die Identität prüft

Was wird kontrolliert?

- Wer? (Identität des Zutrittberechtigten)
- Wann? (Zeitpunkt und Dauer)
- Wo? (Welcher Raum oder Bereich)

NIS 2-Anforderung

NIS 2 fordert dokumentierte, überprüfbare Zutrittskontrollen für alle kritischen Bereiche. Das heißt: Es muss nachweisbar sein, wer zu welcher Zeit Zugang zu welchen Räumen hatte. Das ist nicht verhandelbar und nicht optional.

Eure Produktlösung: Schließzylinder & Beschläge

- Hochwertige Schließzylinder mit Pick-Resistenz
- Sicherheitsbeschläge gegen Gewalteinwirkung
- Elektronische Schließzylinder mit Audit-Trail (Protokoll wer/wann)
- Hybrid-Systeme: Mechanisch robust + digitale Kontrolle

2. ZUGANG

Definition

Zugang ist die Berechtigung, ein IT-System oder Netzwerk zu nutzen. Es ist die logische/digitale Ebene - nicht mehr physisch, sondern im System selbst.

Detaillierte Erklärung

Zugang ist etwas anderes als Zutritt. Während Zutritt 'Darf ich physisch in den Raum?' regelt, regelt Zugang 'Darf ich mich am System anmelden?'. Ein IT-Zugang ist typischerweise ein Login mit Nutzername und Passwort, eine Multi-Factor-Authentication oder ein Zertifikat. Eine Person könnte physisch im Serverraum stehen - Zutritt gewährt - aber trotzdem keinen Zugang zum System haben, weil sie kein gültiges Login hat. Umgekehrt könnte jemand von zu Hause aus Zugang zum System haben, ohne je Zutritt zum Serverraum zu bekommen.

Praktische Beispiele

- Nutzername + Passwort für ein System
- Multi-Factor-Authentication (SMS-Code, App-Authentifizierung)
- Digitales Zertifikat (X.509)
- Zugangstoken, API-Keys

Was wird kontrolliert?

- Wer? (Identität im System - über Credentials nachgewiesen)
- Wann? (Session-Startzeit, Abmeldung)
- Wo? (Auf welches Netzwerk oder System)

NIS 2-Anforderung

NIS 2 fordert sichere Authentifizierung und Autorisierung. Das heißt: Starke Passwörter, Multi-Factor-Authentication wo sinnvoll, und Audit-Logs, die zeigen wer sich wann angemeldet hat.

Zusammenhang mit euren Produkten

Elektronische Schließzylinder können mit Zugangsmanagement-Systemen verbunden werden. So entsteht ein Hybrid-Modell: Zutritt ist physisch (eure Schließzylinder), Zugang ist digital (das Management-System dahinter).

3. ZUGRIFF

Definition

Zugriff ist das, was eine autorisierte Person mit Daten oder Funktionen tatsächlich tun darf. Es ist die wichtigeste Ebene der Sicherheit.

Detaillierte Erklärung

Zugriff ist die tiefste Kontrollschicht. Eine Person könnte Zugang zum System haben - also angemeldet sein - aber trotzdem nicht auf alle Daten zugreifen dürfen. Zugriff wird geregelt durch Rollen, Berechtigungen und Verschlüsselung. Ein Sachbearbeiter in der Personalabteilung kann vielleicht auf Personalakten zugreifen, aber nicht auf Finanzberichte. Ein IT-Techniker kann vielleicht Systemdateien lesen, aber nicht ändern. Zugriff heißt: 'Was genau darf ich mit den Daten tun?' Lesen? Schreiben? Löschen? Exportieren? Jede dieser Aktionen kann separat kontrolliert werden.

Vergleich: Die 3 Ebenen

Schau dir diese Tabelle an - sie zeigt die Unterschiede auf einen Blick:

Merkmal	Zutrittskontrolle	Zugang	Zugriff
Art	Physisch	Digital / Logisch	Digital / Daten
Frage	Darf ich in diesen Raum?	Darf ich mich am System anmelden?	Darf ich diese Daten sehen/ändern?
Technologie	RFID Schlüssel, Karte, PIN, Biometrie	Passwort, MFA, Zertifikate, OAuth	RBAC, ABAC, Verschlüsselung
Beispiel	Tür zum Serverraum öffnet sich mit RFID Schlüssel	Login 'admin' mit Passwort + Code	Admin sieht Daten, Normal-User nicht
NIS 2	Dokumentierte Kontrolle	Sichere Authentifizierung	Least Privilege Principle

Praktisches Szenario: Ein realistisches Beispiel

Szenario: Anna ist Sicherheitsingenieurin bei einem Stromversorger

Schritt 1: Zutrittskontrolle

Anna kommt zur Kontrollzentrale. An der Tür ist ein Schließzylinder mit Pick-Resistenz. Sie steckt ihren Schlüssel rein - die Tür öffnet sich. Zutrittskontrolle erfolgreich. Das System protokolliert: 'Anna, 09.05.2026, 09:15 Uhr, Raum K5-Zentrale'.

Schritt 2: Zugang

Anna setzt sich an einen Computer in der Zentrale. Der Bildschirm zeigt ein Login-Fenster. Sie gibt ihren Nutzernamen 'anna.mueller' und ihr Passwort ein. Zusätzlich authentifiziert sie sich mit einer App auf ihrem Handy. Zugang erfolgreich. Sie ist jetzt im System angemeldet.

Schritt 3: Zugriff

Anna öffnet das SCADA-System (Leitsystem). Sie kann Messdaten ansehen und Status-Reports lesen. Aber sie kann keine Konfiguration ändern - das darf nur ein Senior-Engineer. Sie versucht trotzdem, eine Einstellung zu ändern. Das System blockiert das. Zugriffskontrolle funktioniert: Anna hat Lesezugriff, aber keinen Schreibzugriff.

Das Problem ohne diese Kontrollen:

- Keine Zutrittskontrolle: Ein Eindringling könnte physisch eindringen.
- Kein Zugang: Der Eindringling könnte nicht am System arbeiten (gut).
- Kein Zugriff: Selbst Mitarbeiter könnten Daten manipulieren, die sie nicht ändern sollten.

Alle drei Ebenen sind notwendig. Das ist das Defense-in-Depth-Prinzip: mehrere Schichten, nicht eine.

Ihr habt Fragen zu dem Thema? Hier werden Ihr beraten.