erhardt nxt

NIS2 in der Praxis

Warum Print & Scan-Lösungen oft durchs Sicherheitsraster fallen



Die Rolle von Druck- & Kopie-Systemen für NIS2

Praxisnahes Whitepaper für IT-Leiter & Administratoren

Moderne Drucksysteme sind vollwertige, netzwerkbasierte IT-Systeme. Sie verfügen über eigene Betriebssysteme, sind in Unternehmensnetzwerke eingebunden, kommunizieren mit Mailservern, Verzeichnisdiensten, Cloud-Diensten sowie Management-Systemen und verarbeiten dabei sensible Informationen.

Damit geraten Druck- und Scan-Systeme zunehmend in den Fokus von Anforderungen wie NIS2. Denn die Richtlinie betrachtet nicht nur klassische IT-Systeme wie Server oder Clients, sondern alle Netz- und Informationssysteme, deren Ausfall oder Kompromittierung Risiken für den Geschäftsbetrieb verursachen kann.

Druck- und Scan-Systeme erfüllen diese Kriterien längst. Trotzdem werden sie in vielen Unternehmen noch immer primär als Bürogeräte betrachtet und nicht konsequent in Sicherheits-, Monitoring- und Compliance-Prozesse eingebunden.

Dieses Whitepaper zeigt auf:

- warum Drucksysteme für NIS2 relevant sind
- welche Anforderungen sich daraus ergeben
- welche Rolle Zertifikate dabei spielen
- wie Unternehmen typische Sicherheits- und Compliance-Lücken systematisch schließen können

NIS2 auf einen Blick

NIS2 verpflichtet als europäische Richtlinie zur Verbesserung der Cybersicherheit kritischer und wichtiger Einrichtungen betroffene Unternehmen dazu, Risiken ihrer Netz- und Informationssysteme zu bewerten, geeignete technische, organisatorische und operative Maßnahmen zum Schutz umzusetzen und deren Wirksamkeit nachweisen zu können.

Für IT-Verantwortliche ergeben sich daraus vor allem folgende Fragen:

- **Welche Systeme sind im Einsatz?**
- **Welche Risiken ergeben sich daraus?**
- **Wie werden diese Risiken kontrolliert und dokumentiert?**

„Im Rahmen von NIS2 beschäftigen sich viele Unternehmen intensiv mit Servern, Firewalls oder Endpoints. Drucksysteme werden dagegen oft erst dann betrachtet, wenn es zu operativen Problemen kommt. Dabei sind sie längst Teil der vernetzten IT-Infrastruktur und spielen eine wesentliche Rolle im Kontext von Sicherheit, Compliance und Risikomanagement.“



Marc Fischer
Geschäftsführer bei Erhardt NXT

Drucken im Kontext von NIS2

Lange Zeit wurden Druck- und Multifunktionssysteme vor allem als Arbeitsmittel betrachtet: Sie drucken, kopieren und scannen Dokumente. Entsprechend standen Aspekte wie Verfügbarkeit, Druckqualität oder Betriebskosten im Vordergrund. Als sicherheitsrelevant galten vor allem Server, Clients, Netzwerkkomponenten oder geschäftskritische Anwendungen.
Heute müssen jedoch zusätzlich Anforderungen an **IT-Sicherheit, Compliance, Dokumentation und Risikomanagement** berücksichtigt werden. Der Grund dafür liegt nicht in der Druckfunktion selbst, sondern in der **zunehmenden Integration dieser Systeme** in Geschäftsprozesse und IT-Infrastrukturen.

▸ NIS2 fordert den Blick auf das Gesamtsystem.

Drucksysteme im Wandel

Drucksysteme früher	Drucksysteme heute
Fokus auf Verfügbarkeit	Fokus auf Effizienz, Compliance und IT-Sicherheit
Lokales Ausgabegerät	Vernetzte IT-Komponente mit eigenem Betriebssystem
Drucken & Kopieren als losgelöste Einzelschritte	Integriert in komplexe Geschäftsprozesse
Isolierte Systeme und Einzelkomponenten	Integriert in Active Directory, Cloud- und Fachanwendungen, erreichbar über Protokolle wie HTTPS, SMTP, SNMP sowie APIs
Begrenzter Datenaustausch und geringe Sicherheitsrelevanz	Schnittstelle für sensible Datenströme (z. B. Scan-to-Mail, Dokumentenverarbeitung)
Reaktive Fehlerbehebung und isolierte Verwaltung	Kontinuierliches Monitoring und Lifecycle-Management

Drucken im Kontext von NIS2



Aus dieser Entwicklung ergeben sich Anforderungen, die viele Unternehmen bisher eher von Servern, Clients oder Netzwerkkomponenten kennen.

Anforderungen

1. Transparenz
2. Risikoanalyse
3. Kommunikationssicherheit
4. Volle Kontrolle und Überwachung
5. Nachweisbarkeit

Ableitungen für die IT

Von Anforderung zur Umsetzung

Die entscheidende Frage lautet nun: Wie lassen sich diese umfassenden Anforderungen effizient umsetzen und im laufenden Alltagsbetrieb standardisiert managen?

Die Antwort liegt nicht in Einzelmaßnahmen. Vielmehr müssen technische, organisatorische und administrative Anforderungen gemeinsam betrachtet werden.

1. **Transparenz schaffen**
   Inventarisierung aller Druck- und Scan-Systeme: Geräte, Standorte, Verantwortlichkeiten, Konfigurationen.
2. **Risiken bewerten**
   Prüfung relevanter Kommunikationswege, Abhängigkeiten sowie Auswirkung von Ausfällen.
3. **Kommunikationssicherheit gewährleisten**
   Für Verbindungen zwischen Druckern, Usern, Servern, Diensten, APIs und weiteren Systemen.
4. **Monitoring etablieren**
   Sicherheitsrelevante Zustände kontinuierlich überwachen: Gerätestatus, Konfigurationen, Laufzeiten und Vorfälle.
5. **Nachweisbarkeit sicherstellen**
   Nachvollziehbare Dokumentation umgesetzter Maßnahmen, Zuständigkeiten und Änderungen.

Kommunikationssicherheit im Blick

Eine besondere Herausforderung stellt die Kommunikationssicherheit dar. Sie muss fortlaufend verwaltet, überwacht und aktualisiert werden. Die gesamte Kommunikation moderner IT-Systeme basiert auf **TLS/SSL-Verschlüsselung.** Drucker sind hier keine Ausnahme. Die IT muss sicherstellen, dass Kommunikationspartner eindeutig identifizierbar sind, Verbindungen verschlüsselt erfolgen und Daten unterwegs nicht manipuliert werden können.

Typischer Kommunikationspfad



Zertifikate schaffen Vertrauen

Die technische Basis vertrauensvoller Kommunikation bilden Zertifikate. Sie ermöglichen die eindeutige Identifikation und machen Vertrauenswürdigkeit zwischen Benutzern, Drucksystemen und angebundenen Diensten nachweisbar. Im praktischen Betrieb übernehmen Zertifikate dabei **drei zentrale Funktionen**:

1. **Transportverschlüsselung**
   Schützt Kommunikationswege vor unbefugtem Mitlesen und senkt das Risiko für Man-in-the-Middle-Angriffe.
2. **Authentifizierung**
   Stellt sicher, dass Kommunikationspartner eindeutig identifizierbar sind und ihre Identität nachweisen können.
3. **Integrität der Kommunikation**
   Schützt Daten vor unbemerkten Veränderungen während der Übertragung.

Verschlüsselte Verbindungen basieren auf Zertifikaten. Sie machen Vertrauen technisch messbar.

Zertifikate in der Praxis

Zertifikat ist nicht gleich Zertifikat. Je nach Herkunft unterscheiden sich diese hinsichtlich **Vertrauensniveau, Einsatzbereich und Nachweisbarkeit** erheblich.

Die Wahl des Zertifikats beeinflusst also unmittelbar, wie sicher, nachvollziehbar und effizient Kommunikationsbeziehungen betrieben werden können.

Die wichtigsten Zertifikatsarten

Externe Zertifizierungsstellen (Public CA)

Sie sind global vertrauenswürdig, durch unabhängige Stellen validiert sowie auditierbar.
Stärke: Hohe Vertrauenswürdigkeit ohne eigene PKI-Infrastruktur.
Einsatz: Externe Kommunikation und öffentlich erreichbare Dienste.

Interne PKI (Private CA)

Fungieren als unternehmenseigene Vertrauensinstanz, sind zentral steuerbar & skalierbar. Auditierungen sind intern möglich.
Stärke: Volle Kontrolle über Zertifikate und Prozesse.
Einsatz: Interne IT-Systeme und Unternehmensnetzwerke.

Selbstsignierte Zertifikate (self-signed)

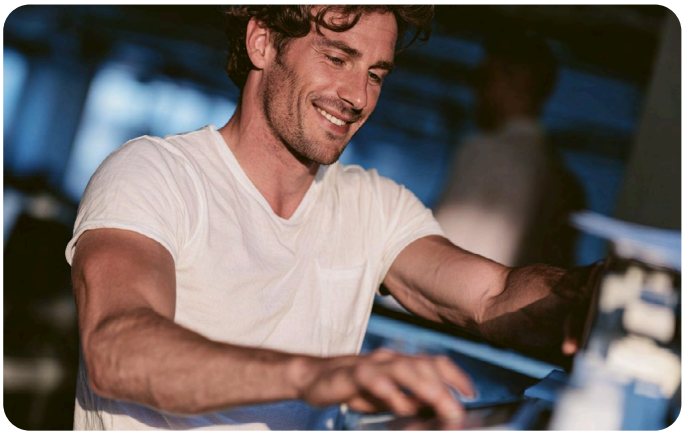
Werden direkt vom System erzeugt, bilden daher keine Vertrauensinstanz und schaffen keine zentrale Steuerung.
Grenzen: Bieten zwar Verschlüsselung, erschweren Nachvollziehbarkeit und einheitliche Governance.
Einsatz: Werkseinstellungen oder Einzelinstallationen.

Zertifikatsmanagement

Neben dem Einsatz der Zertifikate ist auch deren umfassendes Management entscheidend. Denn ein Zertifikat allein schafft noch keine dauerhaft sichere Kommunikation. Nur wenn Unternehmen wissen, welche Zertifikate im Einsatz sind, wer sie verwaltet und wann sie auslaufen, lassen sich Risiken nachvollziehbar steuern und dokumentieren.
Hierzu braucht es geeignetes Zertifikatsmanagement.

Was Zertifikatsmanagement leisten muss

- Übersicht aller Zertifikate erstellen
- Bewertung von Gültigkeit & Trust-Score
- Monitoring von Laufzeiten
- Strukturierter Rollout
- Dokumentation & Protokollierung



Die operative Realität

Wenn Zertifikatsmanagement fehlt, entstehen schnell Risiken. Kritisch wird es dort, wo Unternehmen nicht wissen, welche Zertifikate im Einsatz sind, wann sie ablaufen und wer für sie verantwortlich ist. Ohne zentrale Übersicht, klare Prozesse und Monitoring entstehen Lücken, die sich auf Sicherheit, Compliance und den laufenden Betrieb auswirken können.

Typische Lücken im Alltag

Fehlende Transparenz	Fehlende Prozesse	Fehlende Integration	Fehlendes Monitoring
Häufig fehlt eine zentrale Übersicht zu eingesetzten Zertifikaten. Damit sind Gültigkeitsstatus und Laufzeiten ungewiss, Verantwortlichkeiten unklar.	Zertifikate werden manuell gepflegt und oft erst bei akutem Bedarf erneuert. Ohne Lifecycle-Management ist der Verwaltungsaufwand enorm.	Drucksysteme sind nicht in die PKI eingebunden, es fehlen Verknüpfungen zu integrierten Security-Prozessen, es entstehen isolierte Strukturen.	Abgelaufene Zertifikate oder Konfigurationsprobleme werden oft erst bei Ausfällen erkannt; dann wird nur noch reagiert statt präventiv gemanaged.

Wenn Zertifikatsmanagement fehlt

Diese Lücken sind zunächst organisatorisch. Sicherheitsrelevant werden sie, wenn daraus nicht vertrauenswürdige Kommunikationsbeziehungen, fehlende Nachweisbarkeit oder gestörte Prozesse entstehen.

⚠ Sicherheitsrisiken

Fehlende Authentizitätsprüfungen und nicht vertrauenswürdige Kommunikationsverbindungen erhöhen die Anfälligkeit für Man-in-the-Middle-Angriffe. Datenströme können manipuliert, sensible Informationen abgegriffen oder System- und Benutzeridentitäten kompromittiert werden.

⚠ Compliance-Risiken

Wenn Zertifikate, Laufzeiten und Vertrauensketten nicht dokumentiert oder überwacht werden, fehlt die Nachweisbarkeit. Dadurch steigt das Risiko von Audit-Feststellungen sowie Verstößen gegen Compliance- und NIS2-Anforderungen.

⚠ Operative Risiken

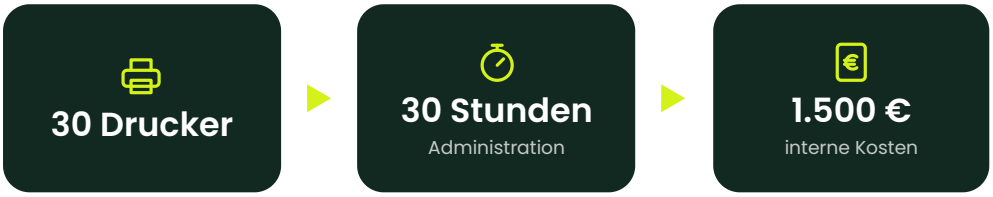
Abgelaufene Zertifikate oder fehlende Trust-Beziehungen können Scan-Vorgänge, API-Kommunikation und andere Prozesse beeinträchtigen. Die Folgen reichen von Funktionsstörungen einzelner Systeme bis hin zu kompletten Ausfällen.

Ohne Management werden Zertifikate schnell von einer Sicherheitsmaßnahme zum Betriebsrisiko.

Die wirtschaftliche Dimension

Aus der Praxis

Fehlendes Zertifikatsmanagement ist nicht nur ein technisches Detail. Es erhöht die Fehleranfälligkeit und erschwert den Nachweis sicherheitsrelevanter Maßnahmen. Doch auch rein manuell umgesetztes Zertifikatsmanagement bindet IT-Ressourcen. In der Praxis entsteht der größte Aufwand dort, wo Zertifikate **händisch gepflegt, Laufzeiten nicht überwacht und Verantwortlichkeiten nicht klar geregelt sind**. Bereits eine überschaubare Druckerflotte kann relevanten Administrationsaufwand erzeugen. Zertifikate müssen geprüft, erneuert, dokumentiert und bei Bedarf neu ausgerollt werden. Eine Vielzahl an Maßnahmen ist erforderlich, ohne dass daraus strategischer Mehrwert entsteht.



Die sichtbaren Kosten sind dabei nur ein Teil des Problems. Kritischer sind die Risiken, die im Hintergrund entstehen: ablaufende Zertifikate, fehlende Transparenz und mangelnde Nachweisbarkeit.

Ohne Übersicht über Zertifikate, Laufzeiten und Zuständigkeiten lassen sich Risiken nicht zuverlässig steuern. Gleichzeitig wird es schwieriger, Aufwand, Ausfälle und Maßnahmen nachvollziehbar zu bewerten.

Zum integrierten Zertifikatsmanagement

Die Lösung liegt nicht darin, Zertifikate dauerhaft manuell zu verwalten. Entscheidend ist, einmalig eine belastbare Grundlage zu schaffen: mit einer **vollständigen Übersicht** aller Zertifikate, **klaren Verantwortlichkeiten, definierten Prozessen** und einer **nachvollziehbaren Dokumentation**.

Für den laufenden Betrieb sollten Monitoring- und Management-Lösungen eingesetzt werden, die Laufzeiten überwachen, Prozesse standardisieren und frühzeitig auf Abweichungen oder Risiken hinweisen. Der Aufwand sinkt, IT-Ressourcen werden frei, Risiken früher erkannt und die Nachweisbarkeit für NIS2 deutlich vereinfacht.

Einmal sauber aufsetzen. Danach überwachen, standardisieren und kontrolliert betreiben.

Fazit

Druck- und Scan-Systeme sind heute Teil vernetzter IT-Infrastrukturen. Damit gehören sie in die Sicherheits-, Risiko- und Compliance-Betrachtung jedes Unternehmens.

Im Kontext von NIS2 reicht es nicht aus, dass diese Systeme funktionieren. Sie müssen transparent, sicher, überwacht und nachvollziehbar betrieben werden. Zertifikate schaffen dabei die technische Vertrauensbasis. Entscheidend ist jedoch nicht das einzelne Zertifikat, sondern die Kontrolle über Systeme, Kommunikationswege und deren sicheren Betrieb.

erhardt nxt

Die IT-Checkliste

Drucksysteme NIS2-ready

- **Transparenz**: Schaffen Sie eine vollständige Übersicht aller Systeme und inventarisieren Sie Ihre Zertifikate. Dokumentieren Sie Verantwortlichkeiten sowie wichtige Kommunikationsprozesse.
- **Monitoring**: Überwachen Sie konsequent alle Laufzeiten und integrieren Sie Alerting bei erkannten Risiken. Erfassen Sie alle sicherheitsrelevanten Ereignisse zentral.
- **Dokumentation**: Setzen Sie auf revisionssichere Nachweise und stellen Sie die Auditfähigkeit sicher. Halten Sie hierfür Zertifikatsstatus und Laufzeiten zentral vor.
- **Automatisierung**: Automatisieren Sie wiederkehrende Verwaltungsaufgaben. Überwachen Sie Zertifikatslaufzeiten softwaregestützt. So reduzieren Sie manuelle Eingriffe und schaffen skalierbare Prozesse.
- **Standardisierung**: Binden Sie Geräte in Ihre interne PKI oder zentrale CA ein. Vereinheitlichen Sie Rollout-Prozesse und vermeiden Sie self-signed Zertifikate.

Wer Transparenz, Monitoring, Standardisierung, Automatisierung und Nachweisbarkeit etabliert, schafft die Grundlage für einen kontrollierten und NIS2-konformen Betrieb von Druck- und Scan-Systemen.

Ihr Kontakt bei Fragen

Wir unterstützen Unternehmen bei der Analyse von Druckumgebungen, der Bewertung bestehender Zertifikatsstrukturen sowie bei der Umsetzung von Sicherheits- und Compliance-Anforderungen.



▶ Termin vereinbaren

Oder Sie besprechen Ihre Fragen direkt persönlich mit Marc Fischer
Schreiben Sie mir: m.fischer@erhardt-nxt.de