



CRA-Konformität für Zutrittslösung



dormakaba 

Noser Engineering war in der Lage, uns als kompetenter und flexibler Sparring-Partner für komplexe CRA-Diskussionen zur Verfügung zu stehen. Und dies zu einem Zeitpunkt, wo europaweit noch sehr grosse Ungewissheit geherrscht hat. Dadurch waren wir frühzeitig in der Lage, unsere Produkte zielgerichtet zu analysieren und Massnahmen einzuleiten, um auch zukünftig als Leader im Access Control Business liefern zu können.

Bertram Weckmann, Senior Manager Software Development, dormakaba Schweiz AG

Das Projekt in Kürze

Noser Engineering unterstützte dormakaba dabei, die Anforderungen des Cyber Resilience Acts konkret, strukturiert und umsetzbar zu machen. Im Fokus standen eine fundierte Bedrohungs- und Risikoanalyse für das exos-System, ein klar risikobasierter Priorisierungsansatz sowie eine realistische Roadmap zur schrittweisen CRA-Konformität.

Ausgangslage

Der Cyber Resilience Act stellt neue Anforderungen an Hersteller vernetzter Produkte. Für dormakaba als führendes Unternehmen im Bereich Zutrittslösungen ist dies besonders relevant, da physische Sicherheit und digitale Sicherheit immer stärker zusammenwachsen.

Ziel

dormakaba wollte den eigenen CRA-Reifegrad fundiert bestimmen und klären, welche technischen, organisatorischen und dokumentarischen Massnahmen für eine effiziente, risikobasierte Umsetzung erforderlich sind.

Lösung

Noser Engineering erarbeitete gemeinsam mit dormakaba einen vollständigen Systemkontext, modellierte relevante Datenflüsse, führte eine strukturierte Bedrohungsanalyse durch und leitete daraus priorisierte Handlungsempfehlungen sowie eine CRA-Roadmap ab.

Ergebnis

dormakaba verfügt über ein belastbares Threat Model als methodische Basis für die weitere CRA-Umsetzung, klare Entscheidungsgrundlagen für Management und Entwicklung sowie eine priorisierte Roadmap für die nächsten Schritte.

Ausgangslage: Regulatorische Anforderungen treffen auf sicherheitskritische Produkte

Der Cyber Resilience Act verpflichtet Hersteller vernetzter Produkte dazu, Cybersicherheit über den gesamten Produktlebenszyklus hinweg nachzuweisen. Für dormakaba besitzt dieses Thema zentrale Bedeutung: Systeme, die physische Sicherheit gewährleisten, müssen auch digital höchsten Schutzanforderungen genügen. Das Unternehmen verfolgte deshalb das Ziel, die CRA-Vorgaben nicht nur formal zu erfüllen, sondern die Sicherheitsarchitektur des eigenen Produktportfolios gezielt weiterzuentwickeln. Im Fokus stand das Kernsystem exos sowie angebundene Komponenten wie Access Manager und Reader.

Bei der konkreten Interpretation und Umsetzung der regulatorischen Anforderungen bestanden jedoch offene Fragen. Welche Komponenten sind in welchem Umfang betroffen? Welche Dokumentation ist erforderlich? Welche Sicherheitsmassnahmen sind regulatorisch notwendig, technisch sinnvoll und wirtschaftlich vertretbar? Noser Engineering brachte in dieser Situation die notwendige Kombination aus Security-Know-how, Architekturverständnis und regulatorischer Umsetzungskompetenz ein.

Ziel: Eine belastbare Standortbestimmung zur CRA-Konformität

Im Zentrum des Projekts stand eine fundierte Standortbestimmung: Wo steht dormakaba in Bezug auf die CRA-Konformität, und welche Massnahmen sind erforderlich, um die regulatorischen Anforderungen effizient und risikobasiert zu erfüllen?

Die wichtigsten Ziele waren:

- Bewertung des aktuellen CRA-Reifegrads
- Definition der relevanten Systemgrenzen
- Identifikation zentraler Assets, Schnittstellen und Datenflüsse
- Durchführung einer strukturierten Bedrohungs- und Risikoanalyse
- Ableitung priorisierter Massnahmen
- Aufbau einer methodischen Grundlage, die dormakaba künftig eigenständig weiterführen kann
- Entwicklung einer realistischen Roadmap zur schrittweisen CRA-Konformität

Herausforderung: Komplexe Anforderungen, grosses Produkt-Ökosystem und hoher Zeitdruck

Der Cyber Resilience Act ist ein umfangreiches Regelwerk mit vielen Facetten. Neben technischen Sicherheitsanforderungen spielen auch Dokumentationspflichten, Nachweispflichten, organisatorische Prozesse und Meldepflichten eine wichtige Rolle.

Gleichzeitig betreibt dormakaba ein grosses und über Jahre gewachsenes Produkt-Ökosystem. Es galt deshalb zu klären, welche Systeme, Komponenten, Schnittstellen und Datenflüsse für die CRA-Betrachtung relevant sind und wo regulatorisch sowie technisch die grössten Risiken liegen.

Eine weitere Herausforderung war der zeitliche Druck. Bestimmte Sicherheits- und Dokumentationsmassnahmen sind aufwändig in der Umsetzung und müssen frühzeitig geplant werden. Die Aufgabe bestand daher darin, aus der Vielzahl möglicher Anforderungen die richtigen Schwerpunkte abzuleiten und einen realistischen, umsetzbaren Fahrplan zu entwickeln. Noser Engineering unterstützte dormakaba genau an dieser Schnittstelle: mit methodischer Klarheit, technischer Tiefe und einem pragmatischen Blick auf die Umsetzbarkeit.

Vorgehen: Vom Systemkontext zum strukturierten Threat Model

Gemeinsam mit dormakaba arbeitete sich Noser Engineering systematisch durch die CRA-Anforderungen und überführte sie in ein konkretes Vorgehensmodell.

Zunächst wurden die relevanten Systemgrenzen definiert. Anschliessend identifizierte das Projektteam zentrale Stakeholder, Assets, Schnittstellen und Datenflüsse. Auf dieser Basis entstand ein vollständiger Systemkontext mit Datenflussdiagramm, der die Grundlage für die weitere Analyse bildete.

Im nächsten Schritt führte Noser Engineering gemeinsam mit dormakaba eine fundierte Bedrohungsanalyse durch. Dabei wurden potenzielle Angriffsvektoren, Risiken und Schwachstellen strukturiert erfasst, bewertet und priorisiert. Der gewählte methodische Ansatz wurde so aufgebaut, dass dormakaba ihn künftig eigenständig weiterführen und auf weitere Systeme übertragen kann. Damit entstand nicht nur eine Projektlösung, sondern ein wiederverwendbares Vorgehensmodell für die weitere CRA-Umsetzung im Produktportfolio.

Die Lösung: Risikobasierte Roadmap zur CRA-Konformität

Aus der gemeinsamen Arbeit entstanden drei zentrale Ergebnisse: ein vollständiger Systemkontext, ein strukturiertes Threat Model und eine priorisierte Roadmap zur CRA-Konformität.

Das Threat Model bildet die erste zentrale CRA-Dokumentationsbasis für das betrachtete System. Es macht transparent, welche Assets geschützt werden müssen, welche Bedrohungen relevant sind und welche Massnahmen mit welcher Priorität umgesetzt werden sollten.

Auf dieser Grundlage formulierte Noser Engineering konkrete Handlungsempfehlungen und identifizierte geeignete Tools und Methoden für die weitere Umsetzung. Der Fokus lag dabei auf einem risikobasierten Ansatz: Sicherheitsmassnahmen werden nicht pauschal definiert, sondern proportional zum tatsächlichen Risiko festgelegt und priorisiert. So entsteht eine CRA-Umsetzung, die regulatorisch belastbar, technisch fundiert und wirtschaftlich sinnvoll ist.

Business Impact: Transparenz, Priorisierung und strategische Sicherheit

dormakaba erhielt durch die Zusammenarbeit mit Noser Engineering eine fundierte Einschätzung des eigenen CRA-Reifegrads und eine belastbare Entscheidungsgrundlage für die nächsten Schritte.

Das erarbeitete Threat Model bildet die methodische Basis für die weitere CRA-Umsetzung und dient zugleich als Referenz gegenüber internen und externen Stakeholdern. Management, Entwicklung, Security-Verantwortliche und Produktteams erhalten damit ein gemeinsames Verständnis darüber, welche Risiken bestehen, welche Massnahmen erforderlich sind und wie diese priorisiert werden sollten.

Der Mehrwert für dormakaba liegt insbesondere in der klaren Priorisierung. Ressourcen können gezielt dort eingesetzt werden, wo sie den grössten Sicherheitsgewinn erzielen. Das reduziert unnötige Aufwände, schafft Transparenz gegenüber regulatorischen Anforderungen und unterstützt eine langfristig robuste Produktstrategie. Gleichzeitig stärkt die strukturierte Vorgehensweise die Innovationsfähigkeit von dormakaba: Sicherheitsanforderungen werden nicht als reine Compliance-Aufgabe behandelt, sondern als integraler Bestandteil moderner, digital vernetzter Zutrittslösungen.

Über den Kunden: dormakaba Schweiz AG

dormakaba ist eines der drei weltweit führenden Unternehmen für Zutrittslösungen. Mit Schweizer Wurzeln seit 1862 und Präsenz in über 130 Ländern bietet das Unternehmen ein breites Portfolio an physischen und digitalen Zutrittssystemen. Dazu gehört unter anderem exos 9300, eine modulare und skalierbare Zutrittskontrolllösung für Grossunternehmen. Mit seinen Lösungen unterstützt dormakaba Unternehmen und Organisationen dabei, Zutritt sicher, effizient und flexibel zu steuern - physisch wie digital.

Benötigen auch Sie Unterstützung für die Umsetzung Ihrer Vision?



Kontaktieren Sie unsere Expert:innen für ein unverbindliches Beratungsgespräch.

Thomas Stadelmann, Quality & Test Services / NI Technologien, +41 79 478 18 33,
thomas.stadelmann@noser.com