NOVO SECURE

Prozessautomatisierung – Aber sicher!

Version: 1.0

Datum: 26.04.2024

www.inovoo.com

INHALTSVERZEICHNIS

1 CYBER-SECURITY – GEHT UNS ALLE AN

Die Bedrohung wächst

Jedes Jahr entstehen durch Cyber-Angriffe enorme wirtschaftliche Verluste. Laut dem Branchenverband Bitkom entstanden im Jahr 2023 Schäden in Höhe von 206 Milliarden Euro durch Cyber-Attacken. Nahezu alle Branchen sind von Angriffen betroffen. Insbesondere im Mittelstand und bei KMU nehmen die Angriffe weiter zu. Acht von zehn Unternehmen waren 2023 von Datenklau, Sabotage oder Spionage betroffen. Hierbei können nicht nur Betriebsunterbrechungsschäden entstehen, sondern auch Verluste durch die Offenlegung von Geschäftsgeheimnissen oder Kundendaten. In vielen Branchen stellt sich nicht mehr die Frage, ob ein Angriff stattfinden wird, sondern wann und mit welchen Auswirkungen.

Einschlägige gesetzliche Regelungen verpflichten Unternehmen, sich so gut wie möglich gegen Cyber-Angriffe zu schützen. Hierbei sind sowohl allgemeine Rechtsnormen (DSGVO, BDSG, StGB etc.) als auch branchenspezifische Regelungen zu beachten (z.B. VAIT/BAIT, IT-Sicherheitsgesetz, SGB, EBA IKT, MA Risk, DORA…).

In den kommenden Jahren ist damit zu rechnen, dass die regulatorischen Anforderungen weiter ausgeweitet werden.

Dem steigenden Risiko stehen somit immer restriktivere gesetzliche Auflagen gegenüber.

Prozessautomatisierung und Cyber-Security

Die Notwendigkeit und Möglichkeiten der Prozessautomatisierung haben einen Einfluss auf das Cyber-Security Risiko eines Unternehmens. Gängige Informationssicherheitssysteme enthalten immer auch das wichtige Element der „Human Firewall“. Eine Sensibilisierung der Mitarbeiter für den Umgang mit eingehenden E-Mails oder Dateien, die über Upload-Links in die Systemwelt des Unternehmens eingebracht werden, kann das Risiko eines Cyberangriffs erheblich senken. Diese Maßnahme ergänzt die vorhandenen Firewalls und die eingesetzte Antivirensoftware.

Um das positive Kundenerlebnis zu verbessern, die Kosten zu kontrollieren, moderne Kommunikationskanäle zu nutzen und Prozesse effizienter zu gestalten, ist eine digitale Prozessautomatisierung - häufig in Verbindung mit KI - unerlässlich. Allerdings ist es dann nur noch eingeschränkt möglich, die 'Human Firewall' zu gestalten und einzusetzen, was das Risiko von Cyber-Attacken erhöht.

Sicherheit bei der automatischen Dateiverarbeitung

Der Prozess der automatischen Dateiverarbeitung hat viele Vorteile, insbesondere bei der Verarbeitung digitaler Eingangskanäle. Er birgt aber auch Sicherheitsrisiken. Dateien aus verschiedenen Kanälen müssen automatisch geöffnet werden. Dabei können auch schädliche Dateien verarbeitet werden, die das unterliegende System potenziell infizieren könnten. Dieses Risiko kann erheblich minimiert werden, indem Dateien vor der automatischen Verarbeitung in einer sicheren Umgebung geöffnet werden.

2 COMPLIANCE BEIM EINSATZ VON NOVO CXP

NOVO CxP - Ihre zukunftsorientiere Automatisierungsplattform

Sie haben sich bereits vor einiger Zeit dafür entschieden, NOVO CxP zur Automatisierung datengetriebener Prozesse einzusetzen. Diese Integrationsplattform automatisiert flexibel die Kundenkommunikation und definierte Geschäftsvorfälle in Ihrem Unternehmen. Dank der echten Omnichannel-Fähigkeit und dem Einsatz von KI sowie der intelligenten Verbindung von IDP und BPM haben Sie die Grundlage für eine zukunftsorientierte IT-Architektur geschaffen. NOVO CxP unterstützt Sie effizient bei der Umsetzung Ihrer Digitalisierungsstrategie gemäß Ihren Prioritäten und Ihrem unternehmensindividuellen Zeitplan. Dank des Low-Code-Ansatzes können Sie weitere Automatisierungsworkflows einfach selbst erstellen und so die Automatisierung in Ihrem Unternehmen sukzessive vorantreiben.

NOVO CxP und Compliance

Aufgrund der Architektur von NOVO CxP, unserer Unternehmensstruktur, unserem aktiven ISMS, unserem Standort und unserer Kenntnis Ihrer Branche sowie der gesetzlichen Anforderungen haben Sie eine Automatisierungsplattform im Einsatz, die Ihren Compliance-Anforderungen voll entspricht.

Wir erfüllen Ihre Datenschutzbedürfnisse, indem wir Daten ausschließlich auf Ihren Servern speichern, transparent über unsere Entwicklungs- und Testgrundsätze informieren, ausschließlich in Deutschland programmieren, DORA-Ready sind und bei unserer Tätigkeit die Anforderungen des SGB erfüllen. Ein an die ISO 27001 angelehntes ISMS stellt sicher, dass wir Ihre und unsere Daten schützen und unsere Dienstleistung auch in Krisensituationen zuverlässig leisten können.

Nun gehen wir noch einen Schritt weiter, um Sie und Ihr Geschäftsmodell zu schützen: Wir haben NOVO Secure entwickelt.

3 DAS CYBER-SECURITY MODUL – NOVO SECURE

NOVO Secure – ihr Sicherheitsnetz bei automatisierten Prozessen

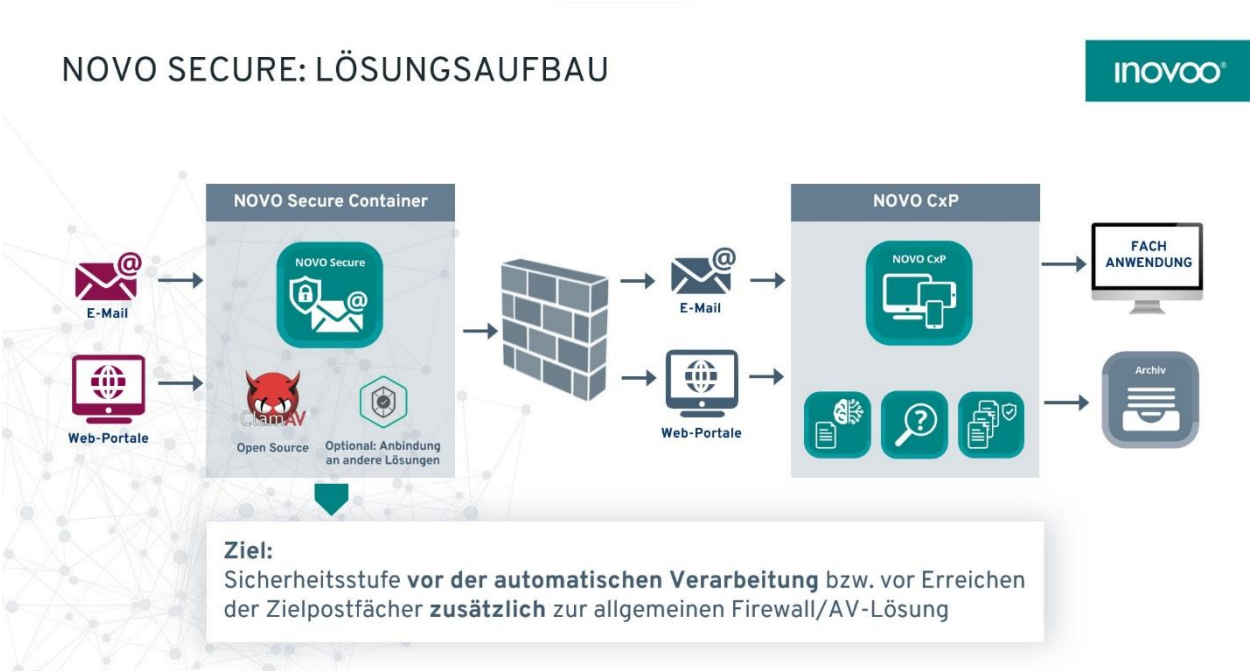
Sie tragen Verantwortung für Ihr Geschäftsmodell, Ihre Mitarbeiter und Ihre Kundendaten. Deshalb optimieren Sie Ihre Geschäftsprozesse mit Hilfe von NOVO CxP. Um Ihnen nun noch mehr Sicherheit gegen Cyber-Angriffe zu geben und die bei der Automatisierung von Multi-Channel-Prozessen wegfallende „menschliche Firewall“ adäquat zu ersetzen, haben wir nun NOVO Secure entwickelt.

- Nachhaltiger und zuverlässiger Schutz vor Cyberangriffen
- Zusätzliche Sicherheitsstufe vor der automatischen Dateiverarbeitung
- Schutz für sensible Unternehmensdaten & Geschäftsprozesse
- Unterstützung von Compliance-Anforderungen durch Implementierung von Sicherheitsstandards
- Einfache und schnelle Integration in bestehenden Workflow
- Zukunftssicher aufgestellt

So funktioniert NOVO Secure

NOVO Secure ist ein Modul, das die Schritte von NOVO CxP simuliert, bei denen Cyber-Risiken auftreten können, bevor die Daten in Ihr System übertragen werden: Öffnen von Dateien und Anhängen, Konvertierung, Export in Fachsysteme u.v.m.

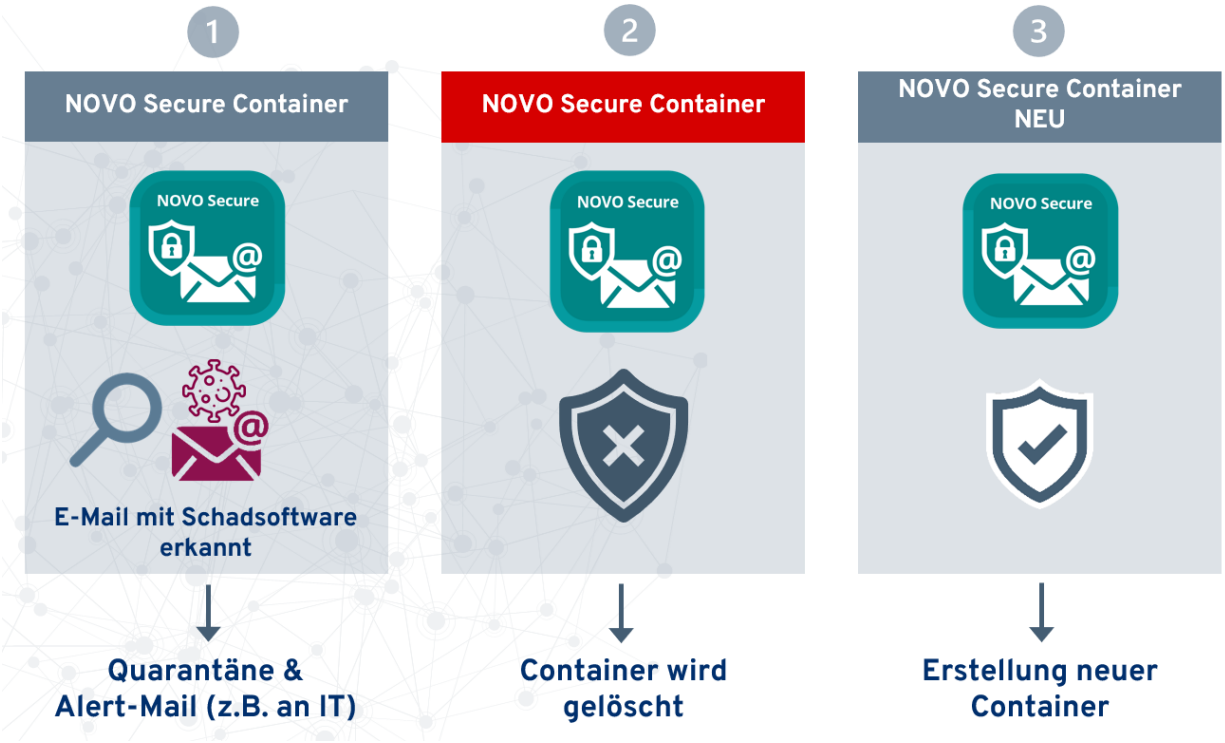
Bevor diese Schritte in Ihrer IT-Umgebung ausgeführt werden, führt NOVO Secure sie in einer Sandbox-Umgebung aus. Ein Virenscanner Ihrer Wahl kann dann auch versteckte Bedrohungen in Anhängen und Dateien erkennen, bevor diese in Ihre Systemumgebung gelangen und dort aktiv werden können.



Beispiel: Eingehende Schadsoftware in einer Email

Im Fall einer eingehenden Schadsoftware wird ein vorab definierter Vorgang aktiviert:

1. Wird eine Bedrohung erkannt, wird sie von NOVO Secure unter Quarantäne gestellt, die IT informiert,
2. der NOVO CxP Secure Container automatisch gelöscht und
3. durch einen neuen NOVO Secure Container ersetzt.



4 LIZENZUMFANG & SYSTEMVORAUSSETZUNGEN

Eine Lizenz für NOVO Secure beinhaltet folgende Funktionen:

- NOVO Secure Container (Sandbox)
- Importer für digitale Eingangskanäle
- Standard-Virenscanner (ClamAV); gegen Aufpreis Integration von weiterer AV-Software möglich
- Exporter in die NOVO CxP Plattform

NOVO Secure wird als Docker-Container ausgeliefert. Unternehmen mit mehr als 250 Mitarbeitenden ODER mehr als 10 Millionen USD Jahresumsatz benötigen ein kostenpflichtiges Abonnement für die kommerzielle Nutzung von Docker Desktop (https://www.docker.com/pricing/).

Die Systemvoraussetzungen richten sich nach den offiziellen Docker-Richtlinien. Diese sind unter folgender URL verfügbar: https://docs.docker.com/desktop/

5 KOSTEN

Die Kosten zur Nutzung der Software ergeben sich aus den folgenden Komponenten:

- Dienstleistung zur Einführung
- Softwarelizenz: 10% der bestehenden Produktivlizenzen (Basislizenz, Funktionserweiterungen und Produktergänzungen), jedoch mindestens 5.000 €

Ein individuelles Angebot erstellen wir Ihnen gerne!

6 KONTAKT

Wir haben Sie überzeugt oder Sie haben Fragen?

Unser Vertriebsteam hilft Ihnen gerne weiter!

inovoo GmbH

Billerberg 11
82266 Inning am Ammersee
T: +49 8143 99957-0
E: sales@inovoo.com

www.inovoo.com

Jetzt E-Mail-Anfrage senden (klick!)