Security-Empfehlungen
für den Einsatz von Komax Maschinen, Software und Dienstleistungen in der Produktion

Inhalt

1 Allgemeine Informationen 2
1.1 Version 2
1.2 Verfügbarkeit der Security-Empfehlungen 2
1.3 Zweck 2
1.4 Geltungsbereich 3
1.5 Rollen und Verantwortlichkeiten 3
1.6 Allgemeine Bemerkungen zum Umgang mit Produkten von Komax 3
1.7 Begrifflichkeiten 4
2 Security-Empfehlungen für den Einsatz von Komax Maschinen, Software und Dienstleistungen 5
2.1 Organisation 5
2.2 Netzwerk und Infrastruktur 7
2.3 Software 8
2.4 Daten und Datensicherung 9
2.5 Kontakt 9
3 Änderungsprotokoll 10
3.1 Versionsverlauf 10
3.2 Änderungen gegenüber der Version 1.0 10

1 Allgemeine Informationen

1.1 Version

Vorliegendes Dokument	Datum	Status
1.1	1. Juni 2025	Freigegeben

1.2 Verfügbarkeit der Security-Empfehlungen

1.2.1 Komax Maschinen

- Online-Hilfe

1.2.2 Online

Die Security-Empfehlungen sind nicht abschliessend und werden laufend aktualisiert. Die jeweils neueste Version kann online bei Komax abgerufen werden.

- Komax (online): https://www.komaxgroup.io/security/de
- Komax (online, QR Code):

1.3 Zweck

Die vorliegenden Security-Empfehlungen dienen dazu, den vernetzten Betrieb von Komax Maschinen in Produktionsanlagen von Komax Kunden sicher und zuverlässig zu gestalten.

Ziel ist es, die Verfügbarkeit der Maschinen hoch zu halten und deren Produktionsfähigkeit gemäss ihrer Spezifikationen zu sichern.

Dabei geht es um die Verhinderung folgender Situationen:

- Unberechtigter Zugriff auf Daten
- Unberechtigte Manipulation von Daten
- Ausführung von unerwünschten oder nicht autorisierten Softwareprogrammen

- Nutzung von Software und/oder Hardware der Maschine für andere als die vom Kunden definierten Zwecke
- Gezielte Funktionsstörung einzelner oder mehrerer Maschinen im Werk mit der Absicht, die Produktion zu stören oder zu verunmöglichen

1.4 Geltungsbereich

Der Kunde trägt zu jeder Zeit selbst die volle Verantwortung dafür, seine Infrastruktur durch geeignete Security-Massnahmen vor Angriffen jeglicher Art angemessen zu schützen, um die einwandfreie Funktion aller Systembestandteile und deren Verfügbarkeit für den produktiven Betrieb aufrecht zu erhalten. Diese Verantwortung schliesst Maschinen, Software und Dienstleistungen von Komax ein.

Die vorliegenden Security-Empfehlungen sind Vorschläge für konkrete Massnahmen, die Komax ihren Kunden zur selbständigen Umsetzung unterbreitet. Sie gelten für alle Maschinen, Software und Dienstleistungen von Komax in der entsprechenden Produktionsanlage des Kunden. Die Umsetzung ist den Kunden überlassen, d.h. nicht zwingend, jedoch dringend empfohlen.

Kunden, die sich in der Umsetzung dieser Security-Empfehlungen nicht sicher sind oder deren Fachkenntnisse bzgl. IT, Computer, Software und Vernetzung nicht ausreichen, ist empfohlen, entsprechende Fachpersonen beizuziehen. Die Verantwortung für die Einrichtung und Umsetzung geeigneter Security-Massnahmen bleibt beim Kunden.

1.5 Rollen und Verantwortlichkeiten

Organisation	Verantwortung
Komax Cluster Product Security	Erstellung, Weiterentwicklung und Pflege der Security-Empfehlungen
Kunde	• Erstellung und Umsetzung von Betriebs- und Security-Konzepten für die OT und IT • Einhaltung des IT-/OT-Betriebskonzepts

1.6 Allgemeine Bemerkungen zum Umgang mit Produkten von Komax

Komax untersagt dem Kunden und jeglichen Drittparteien, in irgendeiner Art und Weise auf die Software oder Maschine einzuwirken, diese abzuändern oder deren Vertragszweck anderweitig eigenhändig abzuändern.

1.7 Begrifflichkeiten

Begriff	Beschreibung	Details
IT	Information Technology	Computerhardware und Softwareprogramme im administrativen Bereich
OT	Operational Technology	Computerhardware und Softwareprogramme zur Überwachung und Steuerung industrieller Anlagen oder physischer Maschinen und ihrer Prozesse
MES	Manufacturing Execution System	Produktionsplanungs- und Steuerungs-system, Leitsystem (Computer und Software)
MIKO	Echtzeit-Datenschnittstelle für Komax Maschinen	Echtzeit-Datenschnittstelle mit drei Hauptbestandteilen • MIKO Discovery: MIKO Server (Maschinen) im Netzwerk finden (basiert auf WS Discovery) • MIKO Publish: Benachrichtigungsservice mit Push-Nachrichten über Events und Statusänderungen (basiert auf MQTT) • MIKO Request: Strukturierter Lese-/Schreibzugang zu allen Daten auf der Maschine (basiert auf REST)
N-S Traffic	North-South-Traffic	Datenverkehr zwischen dem öffentlichen Internet und der Netzwerkinfrastruktur des Kunden
E-W Traffic	East-West Traffic	Datenverkehr zwischen OT und IT
TopImage	Betriebssystem für Komax Maschinen	Betriebssystem auf Basis von Microsoft Windows. Grundlage für die Installation der Bediensoftware Komax HMI oder TopWin.
Komax HMI	Bediensoftware für Komax Maschinen	Software zur Maschinenbedienung durch den Benutzer. Die Software enthält die Bedienelemente und die Ablaufsteuerung der Maschine sowie die Netzwerkverbindung zu übergeordneten Systemen wie z.B. MES.
TopWin	Bediensoftware für Komax Maschinen (frühere Generation, Legacy)	Früher verwendete Software (frühere Generation) zur Maschinenbedienung durch den Benutzer. Diese Software enthält die Bedienelemente und die Ablaufsteuerung der Maschine sowie die Netzwerkverbindung zu übergeordneten Systemen wie z.B. MES.

2 Security-Empfehlungen für den Einsatz von Komax Maschinen, Software und Dienstleistungen

2.1 Organisation

2.1.1 Verantwortliche Person für die interne IT-Security bestimmen. (Analoges Vorgehen wie für die physische Arbeitssicherheit.)

2.1.2 Verantwortliche Person für die Administration der OT bestimmen. (Analoges Vorgehen wie für die Administration der IT.)

2.1.3 Der Administrator Account soll nur für Administrationsaufgaben genutzt werden. Das Administrator-Passwort soll nur durch den Administrator verwendet werden und ist geheim zu halten. Maschinenbenutzer, die keine Administratoraufgaben ausüben, sollen mit einem Benutzer-Account arbeiten, der keine Administrationsrechte besitzt.

2.1.4 Liste der berechtigten Administratoren, deren Verantwortungsbereich und Zugriff auf die Maschine führen und aktuell halten.

2.1.5 Zugang zur Hardware (z.B. Steuerschrank) nur Administratoren erlauben.

2.1.6 Physische Schnittstellen (z.B. USB) nach Möglichkeit nur für Administratoren freigeben oder dedizierte Security-Massnahmen gegen das Einbringen von Schadsoftware einrichten.

2.1.7 Physische Schnittstellen ausschliesslich für die Installation von Komax Software und für die Speicherung von Daten im Fall von betrieblichen oder technischen Problemen verwenden.
Verwendung der USB-Schnittstelle für andere Zwecke sperren, verhindern oder verbieten.

Beispiele: Laden eines Smartphones, Nutzung eines externen Speichermediums (Harddisk, SSD), Verwendung von USB Adaptern für den Anschluss von weiteren Geräten

2.1.8 Softwareinstallationen und Konfigurationsanpassungen (z.B. Betriebssystem) nur den verantwortlichen Administratoren oder Personal von Komax oder deren Partnerunternehmen erlauben. Dazu gehört auch das Geheimhalten und gegebenenfalls regelmässiges Ändern von Passwörtern zu geschützten Bereichen der Software.

2.1.9 Individuelle Passwörter setzen, keine Standard-Passwörter verwenden.

Zu beachten: Das Setzen eines individuellen Passworts für den Administrator-Account hat zur Folge, dass bei Serviceeinsätzen durch Komax oder deren Partnerunternehmen ein Administrator des Kunden den Administrator Account für die nötigen Arbeiten durch einen Servicetechniker an der Maschine freigeben muss. Diese Freigabe kann im Verlauf der Arbeiten mehrfach nötig sein (z.B. bei Neustart der Maschine).

2.1.10 Individuelle Passwörter für jeden Benutzer vergeben und nutzen. Passwörter sind persönlich und somit durch den Benutzer geheim zu halten.

Wenn Passwörter schriftlich festgehalten werden, den Zugang zum Passwortregister einschränken und kontrollieren (z.B. an einer sicheren Stelle lagern, Zugang nur Vertrauenspersonen ermöglichen, resp. erlauben).

2.1.11 Benutzer individuell im MS Windows Active Directory verwalten, Benutzergruppen definieren, Benutzer in Gruppen einteilen.

Beispiele: Spezifische Gruppen für Bediener (Operators), Einrichter, Engineering, Quality Management, Maintenance, Administration

2.1.12 Differenzierte Berechtigungen für die jeweiligen Benutzergruppen auf den Maschinen einrichten (z.B. in Komax HMI).

2.1.13 Wenn keine Unterscheidung der Bediener nötig ist und/oder wenn die Maschine ohne Netzwerkverbindung betrieben wird, kann die Windows-Systemanmeldung von TopImage so konfiguriert werden, dass Windows ohne die explizite Eingabe von Benutzerangaben aufstartet. Die entsprechenden Einstellungen sind für die entsprechenden Maschinen in der Online Hilfe von Komax HMI beschrieben.

Wichtig: Der Kunde trägt zu jeder Zeit selbst die volle Verantwortung dafür, dass die Einstellungen sicher sind und nicht durch Unberechtigte manipuliert werden können.

2.1.14 Internetzugang regulieren.

2.1.15 Betriebssysteme und Konfiguration von Netzwerkelementen, Security Software und Network Group Policies (GPO) sowie Backups stets aktuell halten.

2.1.16 Netzwerktopologie und Konfiguration der Netzwerkelemente protokollieren und Notizen stets aktuell halten. Sicherstellen, dass die Protokolle und Notizen auch in Notfällen verfügbar sind, wenn das Netzwerk, der/die Server und/oder die betroffenen Maschinen nicht verfügbar sind.

2.1.17 Business Continuity Plan/Playbook erstellen und das reibungslose Funktionieren aller Massnahmen in regelmässigen Funktionsprüfungen verifizieren. Sicherstellen, dass die Pläne und Anleitungen auch in Notfällen verfügbar sind, wenn das Netzwerk, der/die Server und/oder die betroffenen Maschinen nicht verfügbar sind.

2.2 Netzwerk und Infrastruktur

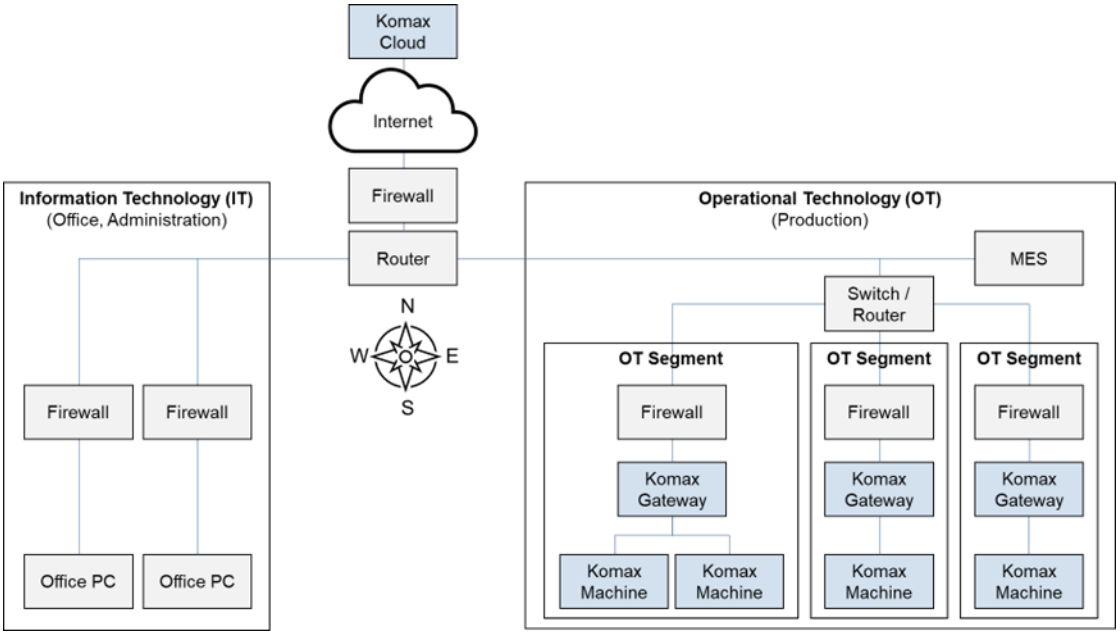
2.2.1 Firewall zur Filterung bzw. Einschränkung der Kommunikation zwischen OT-Netzwerk und Internet verwenden (North-South Traffic).

Nur die minimal notwendigen Verbindungen erlauben:

- Verbindung zur Komax Cloud
- Verbindung auf notwendige Domains zur Durchführung von Softwareupdates
- Dedizierten Remote Access für Servicezwecke ermöglichen

2.2.2 Firewall für die Trennung zwischen Operational Technology (OT) und Information Technology (IT) verwenden (East-West Traffic).

2.2.3 OT-Netzwerk in Segmente aufteilen.
Zu beachten: Durch die Segmentierung sind die Maschinen von ausserhalb des Segments nicht mehr mittels MIKO Discovery auffindbar. Für die Nutzung von MIKO Discovery durch einen zentralen Client muss ein zentrales Register der IP-Adressen der per MIKO angesteuerten Maschinen oder der verwendeten Message-Broker geführt werden.



2.2.4 Komax Gateway verwenden für die Entkopplung des Traffics zwischen Komax Maschinen und den Systemen des Kunden sowie zwischen Komax Maschinen und der Komax Cloud.

Zusätzlich Firewalls einsetzen für die Verbindung ins Internet und zwischen Netzwerksegmenten.

2.2.5 Massnahmen zur Verhinderung und Detektion von Lateral Movement treffen. Massnahmen und Lösungen einrichten, um die Bewegung eines Angreifers innerhalb des angegriffenen Netzwerks zu verhindern oder zu detektieren, z.B. mittels Intrusion Detection System usw.

2.2.6 Wenn im Netzwerk des Kunden Network Group Policies (GPO) verwendet werden, müssen sie in die Windows Registry geschrieben werden, damit vorhandene Einträge überschrieben werden.

Es ist dringend empfohlen, den reibungslosen Betrieb der GPO auf einer einzelnen Komax Maschine mit aktiver Security Software zu prüfen, bevor die GPO im gesamten Netzwerk ausgerollt werden.

Der Kunde ist in jedem Fall selbst dafür verantwortlich, dass die getroffenen Massnahmen die einwandfreie Funktion aller Systembestandteile und deren Verfügbarkeit für den produktiven Betrieb nicht beeinträchtigen.

2.2.7 Resilienz des OT-Netzwerks und aller für die Produktion benötigten Bestandteile (Maschinen, Server, Software, Produktionssteuerungssystem usw.) gegen Denial of Service-Attacken (DoS/DDoS) erstellen.

2.2.8 Ersatzteile und Ersatzgeräte für wichtige Netzwerkelemente und Funktionen vor Ort bereithalten. Aktuelle Betriebssysteme und Anwendungssoftware bereithalten sowie Installationsanleitungen und Konfigurationspläne in schriftlicher Form verfügbar halten. Sicherstellen, dass die Dokumente auch in Notfällen verfügbar sind, wenn das Netzwerk, der/die Server und/oder die betroffenen Maschinen nicht verfügbar sind.

2.3 Software

2.3.1 Information: TopImage wird bei der Auslieferung mit dem zu diesem Zeitpunkt aktuellsten Windows Release ausgeliefert und beinhaltet die Unterstützung für die zu diesem Zeitpunkt aktuellen Komax Computer, Quality Tools usw. Ergänzend dazu stellt Microsoft laufend Windows-Aktualisierungen (Updates, Patches) für TopImage zur Verfügung.

2.3.2 TopImage aktuell halten: Microsoft Updates (Patches) regelmässig via Internet oder lokalen WSUS Server herunterladen und einspielen. Vor jedem Update ein Backup der Maschine erstellen.

Der Update-Prozess für TopImage ist in der Grundeinstellung auf «manuell» eingestellt. Wenn gewünscht, können die Updates auch «automatisch» vorgenommen werden. Der Kunde ist in jedem Fall selbst dafür verantwortlich, die Updates auf mögliche Inkompatibilitäten oder andere Probleme zu testen.

Es ist empfehlenswert, Updates nicht am Patch Day sofort auf allen Maschinen zu installieren, sondern die aktualisierte Software zuerst auf einzelnen Maschinen zu testen und die übrigen Maschinen einen Tag später gestaffelt zu installieren.

2.3.3 Auf Memory Sticks ausgelieferte Komax Software an einer designierten Stelle lagern, Zugriff regeln (z.B. nur für den Administratoren erlauben).

2.3.4 3rd Party Software (z.B. MES Client) nur installieren, wenn betrieblich zwingend notwendig, nur aus verlässlicher Quelle herunterladen und vor der Installation auf deren Integrität prüfen, z.B. mittels Prüfsumme (Hash). Keine private Software installieren. Security-Risiken generell minimieren und die funktionale Verfügbarkeit der Maschine unter keinen Umständen gefährden.

2.3.5 Installierte Security Software verwenden (MS Defender). Security Software regelmässig via Internet oder lokalen WSUS Server aktualisieren und die verfügbaren Updates zeitnah installieren.

2.4 Daten und Datensicherung

2.4.1 Regelmässige Backups erstellen (z.B. wöchentlich), z.B. unter Zuhilfenahme des Database Administration Tools (Komax HMI):

- Datenbank
- Maschinenkonfiguration

2.4.2 Backups an zentraler Stelle ablegen.
Wichtig: Backup niemals ausschliesslich auf der Harddisk der Maschine speichern.

2.4.3 Recovery-Prozess definieren und verifizieren: Vollständiges Recovery anhand der Backups sicherstellen (inkl. Recovery der Betriebs- und Bediensoftware der Maschine). Vollständiges Recovery in regelmässigen Trainingsläufen durchführen, um den problemlosen Ablauf im Ernstfall sicher zu stellen.

2.4.4 Keine privaten oder persönlichen Daten auf der Maschine speichern.

2.5 Kontakt

Kontaktadresse für Fragen und Feedback zu den vorliegenden Security-Empfehlungen:

Komax (online): https://www.komaxgroup.io/security/de

- Komax (online, QR Code):

3 Änderungsprotokoll

3.1 Versionsverlauf

Version	Datum	Status
1.0	1. Juli 2023	Freigegeben
1.1	1. März 2025	Freigegeben

3.2 Änderungen gegenüber der Version 1.0

Abschnitt	Änderung	Inhalt
1.2	Änderung	Verfügbarkeit
2.1.14	Änderung	Neu im Abschnitt 2.1 Organisation
2.1.15	Neu	Überprüfung und Aktualisierung der Massnahmen
2.1.16	Änderung	Neu im Abschnitt 2.1 Organisation
2.1.17	Neu	Business Continuity Plan, Funktionsprüfungen
2.2.3	Ergänzung	Grafik
2.2.4	Ergänzung	Komax Gateway
2.2.5	Neu	Lateral Movement
2.2.6	Änderung	Neu im Abschnitt 2.2 Netzwerk und Infrastruktur
2.2.7	Neu	Resilienz gegenüber DOS und Ransomware-Angriffen
2.2.8	Neu	Ersatzteile und Ersatzgeräte für Netzwerkelemente
2.5	Änderung	Kontaktadresse