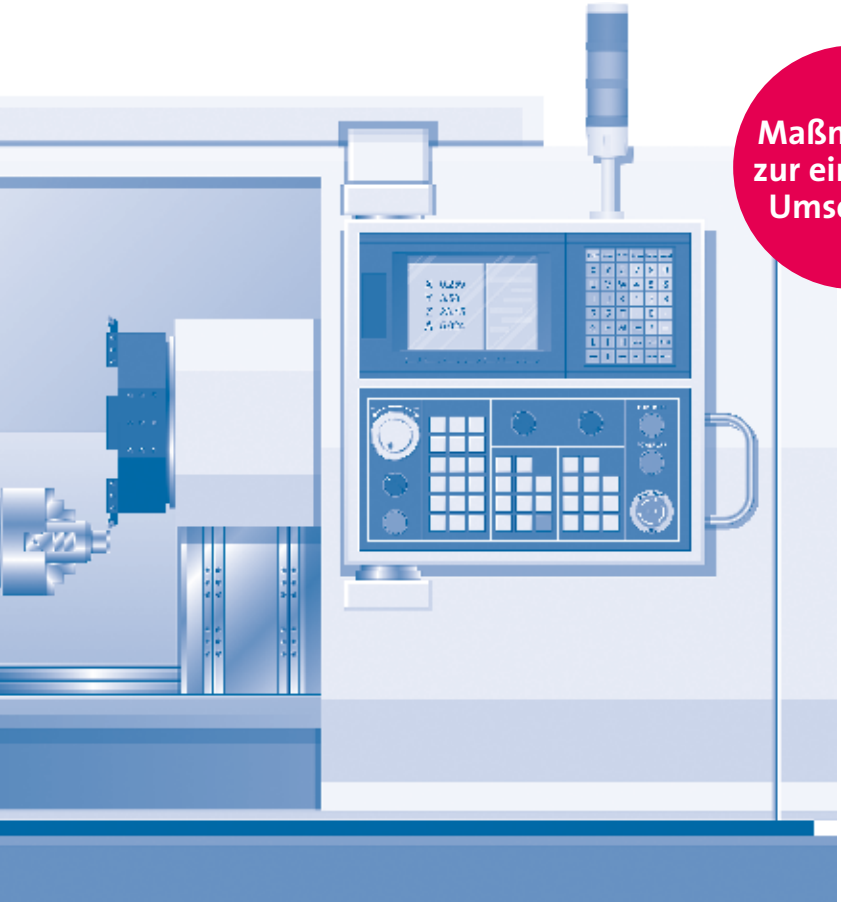
Verein Deutscher Werkzeugmaschinenfabriken

IT-Sicherheit an Werkzeugmaschinen



Maßnahmen zur einfachen Umsetzung

IT-Sicherheit an Werkzeugmaschinen

Systeme zur Fertigungs- und Prozessautomatisierung – zusammengefasst unter dem Begriff **Industrial Control Systems (ICS)** – werden in nahezu allen Infrastrukturen eingesetzt, die physische Prozesse abwickeln. Dies reicht von Energieerzeugung und -verteilung über Gas- und Wasserversorgung bis hin zu Fabrikautomation, Verkehrsleittechnik und modernem Gebäudemanagement. Solche ICS sind zunehmend denselben **Cyber-Angriffen** ausgesetzt, wie dies in der konventionellen IT der Fall ist [1] [14]*.

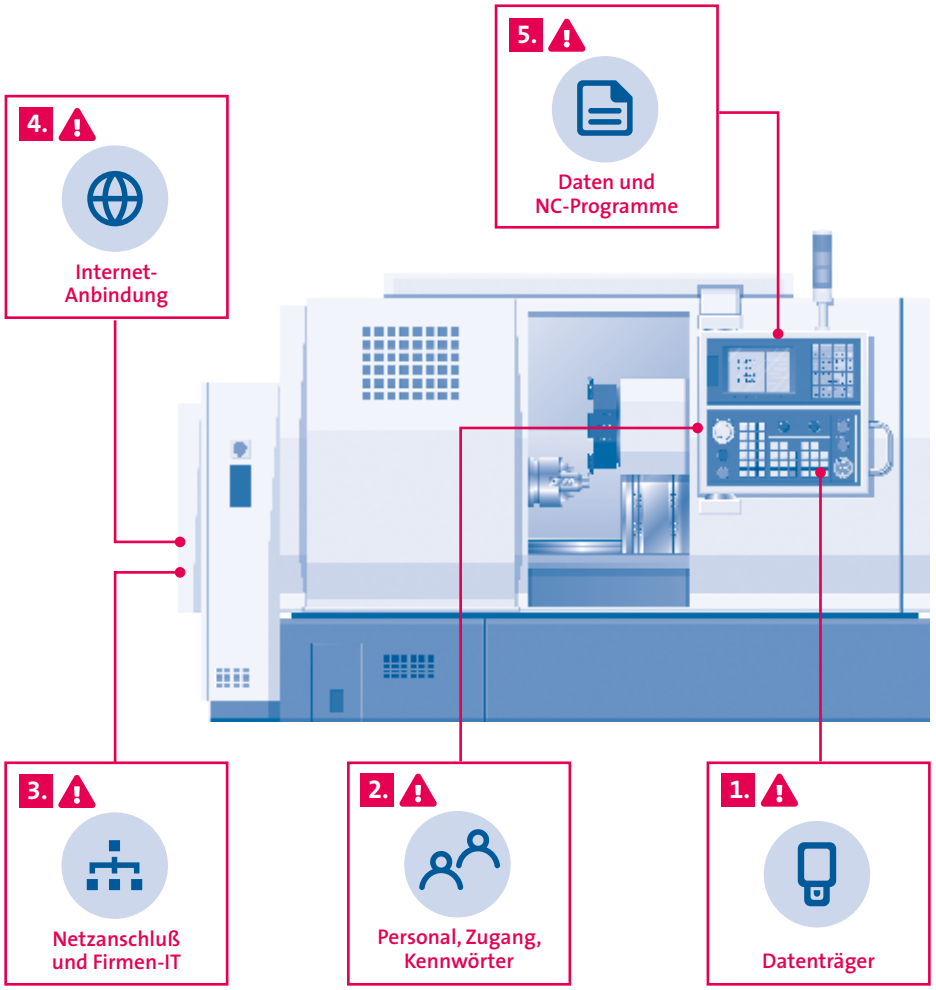
Betreiber solcher Anlagen müssen sich angesichts einer **zunehmenden Häufigkeit von Vorfällen** und neu entdeckten Schwachstellen dringend dieser Thematik annehmen. Dies gilt sowohl für Infrastrukturen, die unmittelbar mit dem Internet verbunden sind, als auch für diejenigen, welche auf mittelbarem Wege durch Cyber-Angriffe attackiert werden können. **Ebenso betroffen sind Maschinen in der Produktion, insbesondere auch Werkzeugmaschinen** [4]. Sich selbst oder sein Unternehmen aus diesem Bedrohungsszenario auszuschließen ist nicht nur fahrlässig, sondern geradezu höchst gefährlich! Die Frage darf nicht lauten, ob ein Angriff erfolgen wird, sondern **wann dieser erfolgt und wie folgenschwer er verlaufen wird** [14].

Die Frage darf nicht lauten, ob ein Angriff erfolgen wird, sondern wann dieser erfolgt und wie folgenschwer er verlaufen wird.

Die **Optimierungspotenziale durch den zunehmenden Einsatz von IT-Technologien im Produktionsprozess** und die Entwicklungsmöglichkeiten in täglichen Unternehmensabläufen sind zu groß, als dass sich wirtschaftlich handelnde Organisationen dem entziehen könnten. Ziel muss es sein, einen möglichst hohen Grad an IT-Sicherheit bei voller Produktivität zu erreichen.

Die nebenstehende Abbildung zeigt eine Übersicht, an welchen Stellen bei Werkzeugmaschinen besondere Beachtung unter dem Gesichtspunkt IT-Sicherheit empfohlen wird.

Primäres Ziel dieses Dokuments ist es, Betreiber von Werkzeugmaschinen **für die Bedrohungen zu sensibilisieren** und **einfache organisatorische und technische Maßnahmen zu zeigen**, mit denen **pragmatisch** die IT-Sicherheit verbessert werden kann – besonders auch an schon vorhandenen Maschinen.



Als **Ausgangspunkt für eine Standortbestimmung** dient i. d. R. eine unternehmensspezifische Risikoanalyse der Cyber-Bedrohungslage. Eine Annäherung kann z. B. über den Fragebogen zur IT-Sicherheit des VDMA [3] erfolgen.

Zugunsten **einfacher Verständlichkeit und Umsetzbarkeit** verzichtet das vorliegende Dokument aber bewusst auf fachlich tiefgehende Erörterungen des Themas IT-Sicherheit, etwa bezüglich der unternehmensweiten Anwendung neuerer Normen wie **IEC 62443** [15]. Für den fachlich Interessierten wird daher zur Vertiefung auf entsprechende Literatur verwiesen.

* Weiterführende Literatur und Informationsquellen: Siehe Seite 13 und 14.

1. Datenträger

Situation heute Wechseldatenträger, **vorrangig USB-Sticks**, sind weit verbreitet. Diese werden für viele unterschiedliche Zwecke eingesetzt – u. a. um **Bearbeitungsprogramme** und weitere Fertigungs- oder Auftragsdaten **auf die Maschine zu übertragen**, aber ebenso als Werbemittel, allgemeines Datenaustauschmedium, Lieferantenkatalog und weiteres. Mitarbeiter im Unternehmen **verwenden diese häufig auch privat**, z. B. um Arbeitsdokumente aus dem Home-Office zu übernehmen. **Fremdpersonal**, wie Wartungspersonal oder andere Dienstleister, nutzt **oft eigene Wechseldatenträger**, welche wiederum mit einer Vielzahl von Anlagen in Kontakt kommen. Als Wechseldatenträger zählen hier auch etwa über den USB-Port an der Maschine angeschlossene Handys. Unternehmen und Anwender sind hinsichtlich der sich daraus ergebenden Bedrohungen häufig **nicht ausreichend sensibilisiert** [1] [5].

Bedrohungen

Datensicherheit: Daten können leicht kopiert und transportiert werden, auch über Unternehmensgrenzen hinweg.

Infektionsgefahr: Durch Kontakt mit vielen Systemen kann über Wechseldatenträger leicht Schadsoftware übertragen und eingeschleppt werden.

Maßnahmen

			organisatorisch
●	●	●	**Regelmäßige Sensibilisierung der Anwender** im Unternehmen, insbesondere auch in der Produktion
●	●	●	Verpflichtung der Belegschaft zu einem **sorgsamen Umgang mit Wechseldatenträgern**
●	●	●	**Bereitstellung unternehmenseigener USB-Sticks zur ausschließlichen Nutzung im Unternehmen**, Verbot der Nutzung privater Wechseldatenträger und des Anschlusses anderer per USB verbundener Datenträger wie portable SSD-Festplatten oder Smartphones im Unternehmen
		●	Regelung mit entsprechender **Freigabe zum Zugriff auf ggf. verriegelte USB-Ports**
			technisch
●	●	●	Nutzung von **ausschließlich unternehmenseigenen**, ggf. personalisierten, und regelmäßig (!) auf Schadsoftware geprüften Datenträgern
	●	○	Übertragung von Programmen auf Maschinen nur mittels **spezieller, dafür reservierter USB-Sticks** über Rechner mit aktuellem (!) Virenschutz
		●	**Einrichtung von Schleusen** mit z. B. (permanent aktualisierten [!]) Virenscannern für Wechseldatenträger
		●	Einschränkung des physikalischen Zugangs zu USB-Schnittstellen

2. Personal, Zugang, Kennwörter

Situation heute Heute **fehlen bei vorhandenen Produktionsmitteln häufig individuelle Zugangsberechtigungen und Passwörter**. Entweder ist gar keine Authentifizierung aktiv und der „Standarduser" hat die Rechte eines Administrators, oder es ist nur ein allgemein bekanntes Passwort zum Schutz vorhanden (z. B. User: „admin", Kennwort: „admin"). Begründet wird diese Nachlässigkeit (= **Sicherheitslücke!**) oft mit dem notwendigen schnellen, unkomplizierten Zugang zu den Geräten, der für eine hohe Anlagenverfügbarkeit sorgen soll. Auch an Werkzeugmaschinen ist teils das **Systemkennwort/ Steuerungskennwort dauerhaft aktiv**, um dem Bediener erhöhte Benutzerrechte einzuräumen. Die Absicherung durch den Berechtigungswahlschalter wird damit umgangen. So können leicht wichtige Bearbeitungsparameter geändert werden, was zu Produktionsmängeln und Maschinenschäden führen kann. Räumlich ist i. d. R. ein Zugang zur Maschine nicht beschränkt oder beschränkbar.

Bedrohungen

Der Zugang zu den Geräten ist oft nicht gesichert. **Jeder kann dann die Geräte bedienen und (um-)programmieren**, NC-Programme laden, anpassen, speichern und löschen, Parameter wie Maschinendaten (Achsbeschleunigungen etc.) ändern usw.

Zusätzlich kann über den Zugang zu einem Gerät oft der **Zugang zu weiteren Geräten, Systemen oder in die gesamte IT-Infrastruktur** des Unternehmens erfolgen.

Maßnahmen

			organisatorisch
●	●	●	**Vertrauliche Behandlung von Kennwörtern!** Auch allgemein bekannte Kennwörter dürfen nur von autorisierten Mitarbeitern genutzt werden
●	●	●	wenn möglich Kennwörter immer **personenbezogen** festlegen
●	●	●	**Sensibilisierung** der Mitarbeiter
○		●	Aufbau und Umsetzung eines **Zugriffs- und Berechtigungs-Systems** (Identity- und Access-Management), z. B. Einsatz **unterschiedlicher Benutzerrechte auch für die Steuerung**, sofern dies vom jeweiligen System unterstützt wird
	●		**Zweckgemäße Nutzung des Berechtigungsschalters** an der Werkzeugmaschine. I. d. R. verfügen Werkzeugmaschinen bereits über einen entsprechenden (Schlüssel-)Schalter, in der Praxis wird dieser nicht immer eingesetzt
			technisch
●	●	●	**Aktivierung und konsequente Nutzung von Authentifizierungen/ Autorisierungen als Zugangsbeschränkungen** wo vorhanden
	●	○	Aktivieren eines **automatischen Ausloggens** bei nicht aktivem Nutzer, keine dauerhaft gesetzten Kennwörter verwenden

Geschäftsleitung · Produktion · IT-Abteilung · ● voll zuständig · ○ teilweise zuständig

3. Netzanschluss und Firmen-IT

Situation heute Um das Potenzial einer vernetzten Fertigung zu erschließen, werden **immer mehr Produktionsmaschinen in das Firmen-Netzwerk (LAN) integriert**. So kann eine Maschine mit einer Fertigungssteuerung (Manufacturing Execution System, MES), der Produktionsplanung (Production Planning System, PPS) oder einem Warenwirtschaftssystem (Enterprise Resource Planning, ERP) kommunizieren, etwa zur Abfrage des Lagerbestands, oder auch, um Produktivitätskenndaten an höhere Ebenen zurückzumelden. Bei Einsatz von MES-Systemen ist der Anschluss an das Firmennetz obligatorisch, es muss jedoch zwingend eine Trennschicht, z. B. Virtual LAN (VLAN), eingesetzt werden. Eine **unbedingt empfehlenswerte Trennung** [1] [7] [9] der verschiedenen Netzwerkbereiche und Zugriffsrechte innerhalb des Unternehmens ist seit langem Stand der Technik, aber längst nicht überall umgesetzt.

Bedrohungen

- Schadsoftware, welche im Büro-IT-Umfeld ins Netz gelangt, kann die **Produktionsmaschinen infizieren oder beeinträchtigen**.
- Personal und ggf. Schadsoftware kann bei unzureichender Absicherung **von der Produktionsmaschine aus auf Geräte und Daten in der Büro-IT zugreifen**.

Maßnahmen

	GL	Prod.	IT	
organisatorisch	●	○	●	Unternehmensweite **Festlegung der notwendigen und sinnvollen Zugriffsrechte** (*„Soll der Drucker der Geschäftsführung wirklich von der Produktionsmaschine aus zu erreichen sein?“, „Kann der Pförtner auf die NC-Programme zugreifen?“* etc.) [2]
technisch	○	●	●	**Beschränkung der Zugriffsrechte** der einzelnen Nutzer und Geräte auf das Sinnvolle und Notwendige
			●	Logische **Trennung der Netzwerksegmente**, also z. B. **Trennung der Produktion vom Rest des Unternehmens** mittels VLAN o. Ä.
			●	Einsatz von **Firewalls**, **Monitoring**-Lösungen etc.
			●	**Eingeschränkter logischer oder physikalischer Zugang** zu LAN-Ports

4. Internet-Anbindung

Situation heute Über eine Anbindung der Firmennetze und auch der Produktionsmaschinen an das Internet werden **zahlreiche Services möglich**, welche sonst entweder gar nicht, nur deutlich teurer oder stark eingeschränkt ermöglicht werden können (etwa Remote-Service [6], betriebswirtschaftliche Anwendungen z. B. für Zahlungsströme, Anbindung an die Kunden-IT für Auftragsinformationen etc.). Ein Schutz der Internet-Anbindung durch eine Firewall wird üblicherweise umgesetzt [4].

Bedrohungen

- **Externer Zugriff auf Systemkomponenten** bei Nutzung von öffentlich bekannten Standardkennwörtern (z. B. User: „admin“, Kennwort: „admin“).
- **Ausnutzung von bekannten Schwachstellen** oder Ausführung sogenannter Zero-Day-Exploits, d. h. bislang unbekannter Angriffe, für die noch keine Erkennungsmöglichkeiten in Anti-Viren-Produkten o. Ä. existieren.
- Einfaches **externes Auffinden von angreifbaren Steuerungskomponenten** des Unternehmens durch entsprechende Suchmaschinen [7].

Maßnahmen

	GL	Prod.	IT	
organisatorisch	●	●	●	Unternehmensweite **Festlegung der notwendigen und sinnvollen Zugriffsrechte** (*„Wer darf was?“*)
		●	●	Personalisierung von Zugängen
technisch			●	Einsatz einer stets aktuellen (!) und regelmäßig gewarteten (!) **Firewall**
	●	●	●	Einsatz von **starken Kennwörtern, wo möglich 2-Faktor-Authentifizierung, und Zertifikate für externe Zugänge**
			●	(Ggf. zeitweise) **Deaktivierung nicht genutzter Dienste** und Features
			●	Logische **Trennung der Netzwerksegmente**, also z. B. **Trennung der Produktion vom Rest des Unternehmens** mittels VLAN

5. Daten und NC-Programme

Situation heute Allgemein liegt eine **steigende Menge unternehmenskritischer Informationen** (nicht nur für die Produktion) entweder ausschließlich oder auch in elektronischer Form vor. Der sorglose Einsatz von Wechseldatenträgern, verbunden mit einem unzureichenden Zugriffs- und Berechtigungssystem, erlaubt den **leichten Zugriff auf Daten** [4]. So lassen sich beispielsweise technische Zeichnungen, Angebote, Aufträge, oder Prozessparameter und NC-Programme ohne großen Aufwand einfach von einem Laufwerk oder einer Maschine auf einen USB-Stick kopieren und in der Tasche aus dem Unternehmen tragen [7] [8]. Eine Nachverfolgbarkeit dieses Datendiebstahls ist – ohne Zugriffs- und Berechtigungssystem – unmöglich.

Bedrohungen

- Datenverlust infolge von **Fehlbedienung** (versehentliches Löschen oder Verschieben).
- Datenverlust durch **Schadsoftware** (z. B. Erpressungs-Trojaner, mittels Phishing etc.).
- Datendiebstahl und **Know-how-Verlust**.

Maßnahmen

			Klassifizierung des **Wertes von Daten und Informationen im Unternehmen**, Regelung zu Umgang, Schutz und Sicherung sowie Vernichtung	organisatorisch
			Erstellung eines Backup-Konzeptes und regelmäßige Datensicherung, auch für Produktionsdaten wie NC-Programme, auch von Bearbeitungsmaschinen	organisatorisch
			Einführung von **standardisierten Abläufen für den Umgang mit Daten** bei **Neueintritt und Ausscheiden** von Mitarbeitern	organisatorisch
			Festlegung von **Zugriffsbeschränkungen** für alle im Unternehmen vorhandenen Informationen (Berechtigungen)	technisch
			Inventarisierung, Personalisierung oder Auflistung (Whitelisting) zugelassener Datenträger im ICS-Netzwerk	technisch
			Datenverschlüsselung bei Übertragung von Daten auf Datenträgern und in Geräten (z. B. PCs)	technisch
			Monitoring und Meldung ungewöhnlicher Datenzugriffe, Verbindungen oder Verbindungsversuche	technisch
			Weitere technische Sicherheitsmaßnahmen wie **Segmentierung** von Netzen, Deaktivierung von Internet-Zugängen, Einrichtung von VPNs, Firewalls etc.	technisch

Glossar IT-Security

Safety und Security

Mit Safety wird i. d. R. die funktionale Sicherheit oder auch Personensicherheit beschrieben. Security bezeichnet hingegen die Absicherung von IT-Anlagen (Datensicherheit).

Safety als gesetzliche Vorgabe bleibt weiterhin relevant. Mit zunehmendem Digitalisierungsgrad der Produktion wird aber begleitend die Datensicherheit (Security) immer wichtiger für einen störungsfreien Betrieb; siehe dazu auch die weiteren Ausführungen in der vorliegenden Veröffentlichung.

Credentials

Zugangsdaten.

Üblicherweise eine Kombination aus Benutzername und Kennwort.

Phishing und Social Engineering

Mittels gefälschter Information (Absender oder Dokumente) wird versucht, an vertrauliche Informationen und Zugangsrechte zu gelangen.

Klassische Beispiele sind E-Mails von vorgeblich bekannten Absendern mit Aufforderungen, ein bestimmtes Dokument zu öffnen (*„Hier ist Ihre Auftragsbestätigung mit der Bitte um Prüfung“*, *„Bitte aktualisieren Sie Ihre Zahlungsinformationen“* etc.). Die Mails werden i. d. R. unter falschem Absender versandt. Die enthaltenen Dokumente oder Links bauen Verbindungen zu Hintergrund-Webseiten auf, laden dann die Schadsoftware unbemerkt auf den Rechner und kompromittieren damit das System: Alles, was der Anwender kann/darf (auf Dateien im Netz zugreifen, löschen etc.), kann/darf der Angreifer dann auch.

IAM (Identity and Access Management)

Verwaltung der Identifikation und der Zugriffsrechte von Nutzern eines Systems.

Getrennte Zugriffsrechte ermöglichen einen nutzerbasierten Zugang zu Daten und Informationen. Beispiele wären etwa ein Windows-Login oder eine ERP-Zugangsberechtigung. Die Softwarekomponente zur Verwaltung der verschiedenen Nutzeridentitäten und deren Zugriffsrechte wird als IAM bezeichnet.

Whitelisting / Blacklisting

Ausschließliches Zulassen (Whitelisting) oder gezielter Ausschluss (Blacklisting) von spezifizierten Geräten, Datenträgern etc.

Über Whitelisting kann z. B. nur bestimmten, gewünschten Geräten der Zugang zum Firmennetz gestattet werden. Über Blacklisting werden z. B. einzelne bekannte und unerwünschte Absender von Werbe-Mails blockiert.

(Zero-Day-)Exploits

Ausnutzung von (ganz neuen) Sicherheitslücken.

Über sogenannte „exploits" werden Sicherheitslücken in Softwarekomponenten ausgenutzt, um in das System einzubrechen. Besonders kritisch sind dabei solche Sicherheitslücken, für die noch kein Patch (Maßnahme) des Herstellers bereitsteht und welche erstmalig ausgenutzt werden, so dass noch keine Schutzsoftware diese erkennen kann („zero day").

Bot-Netz

Ein fremder Rechner (Master) steuert viele dezentrale Rechner (Slaves) mittels dort installierter Schadsoftware fern, i. d. R. unbemerkt vom infizierten Nutzer.

Bot-Netze können auf zweierlei Weise Schaden anrichten: erstens unmittelbar durch die Auslastung der Rechnerleistung, was zu einer Verlangsamung der betroffenen Systeme führt und z. B. eine Maschinensteuerung schwer bedienbar machen kann, und zweitens mittelbar über Handlungen, die vom Master (= Steuerrechner) initiiert, aber im Namen des Slaves (= des infizierten Rechners) ausgeführt werden, z. B. Spam unter Angabe der Adresse der Firma versenden oder Schlimmeres (Urheberrechtsverletzungen, kriminelle Inhalte ...).

DDoS-Angriff

DDoS steht für „Distributed Denial of Service"; eine DDoS-Attacke führt i. d. R. zu massenhaften Anfragen von vielen verschiedenen Geräten („distributed"), welche dann den angegriffenen Dienst/Server überlasten und damit de facto stilllegen.

Um DDoS-Angriffe durchzuführen, benötigt der Angreifer die Kontrolle über eine Vielzahl von Geräten, welche er beispielsweise über ein → **Bot-Netz** erlangen kann. Angegriffen werden häufig Webserver (Ergebnis: *„Seite nicht erreichbar"*), aber auch andere Dienste können Ziel solcher Angriffe werden, z. B. Datenbanken.

Netzwerk-Segmentierung

Trennung eines Netzwerks in mehrere, voneinander logisch getrennte Segmente.

Eine Netzwerk-Segmentierung stellt eine logische (nicht physikalische) Trennung eines großen Netzes in mehrere Sub-Netze dar. So können abgeschottete Bereiche eingerichtet werden, etwa für Produktion und Buchhaltung, ohne neue Netzwerkkabel zu verlegen, ggf. müssen aber Komponenten wie Switches ausgetauscht werden.

VPN (Virtual Private Network)

Virtuelles Netzwerksegment, welches innerhalb eines großen Netzwerks (z. B. Internet) einen geschützten Bereich bereitstellt (z. B. für Zugang zum Firmennetz über das Internet).

Über ein VPN kann eine „sichere Insel" in einer unsicheren Umgebung eingerichtet werden. Ein VPN bindet den Nutzer logisch vollständig (!) in das Netz ein, so dass ohne weitere Maßnahmen alle Aktivitäten möglich sind, welche auch im lokalen Netz erfolgen können.

IPsec, L2TP, OpenVPN, IKEv2, PPTP ...

Protokolle für die Bereitstellung eines VPN, abhängig vom Hersteller (z. B. IPsec bei Cisco).

Die eingesetzten Protokolle hängen vom Hersteller der VPN-Lösung ab.

TLS (Transport Layer Security)

Modernes Verschlüsselungsverfahren, welches u. a. für Webseiten eingesetzt wird (bei https://), Nachfolger von SSL (Secure Sockets Layer).

Wenn Daten unverschlüsselt über das Internet übertragen werden (etwa bei „http://" statt „https://") können die übertragenen Daten von Dritten mitgelesen werden. Aus diesem Grund geben moderne Webbrowser oft eine Warnung aus, wenn noch unverschlüsselte Seiten aufgerufen werden sollen.

OT (Operational Technology)

Beschreibt Produktionsmittel, wird genutzt zur Abgrenzung gegenüber IT (Informationstechnologie).

I. d. R. von IT-Experten genutzter Ausdruck für Produktionstechnik im weiteren Sinne.

IT-Sicherheit betrifft das gesamte Unternehmen

> *„Informationssicherheit ist kein Zustand, der einmal erreicht wird und dann fortbesteht, sondern ein Prozess, der kontinuierlich angepasst werden muss.“*

Diese Aussage ist dem – sehr zur Umsetzung empfohlenen – Dokument **Basis-Absicherung nach IT-Grundschutz** entnommen, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik (BSI) [12] [18]. Praktisch bedeutet dies, dass für die Erlangung von IT-Sicherheit **alle Mitarbeiter und Unternehmensbereiche gefordert** sind [11], von der Geschäftsleitung über die Produktion und die verschiedenen anderen Abteilungen bis hin zu externen Dienstleistern [10]. **Sowohl organisatorische als auch technische Regelungen müssen ineinandergreifen** und ständig den aktuellen Erfordernissen angepasst werden.

Speziell Produktionsmaschinen stellen besondere Anforderungen an das unternehmensweite IT-Umfeld. Sie sind meist **fertig konfigurierte Systeme** vieler verschiedener, eng aufeinander abgestimmter Komponenten, die nicht verändert oder regelmäßig aktualisiert werden können oder sollen. Der technische Hintergrund liegt in den **hohen Zuverlässigkeitsanforderungen** und **der Abstimmung der Softwarekomponenten mit der jeweiligen Hardware**. Auch das Bedieninterface der Maschine (HMI) wird oft an Kundenbedürfnisse angepasst. Änderungen an diesem System wie etwa installierte Virenscanner etc. bedürfen immer der Freigabe des Maschinenherstellers.

Entsprechend muss eine robuste und widerstandsfähige IT-Umgebung in der Produktion solche Maschinen und Anlagen schützen. Einen breiten Überblick und guten Einstieg in das Thema liefern hier beispielsweise der **Leitfaden des VDMA für mittelständische Unternehmen** [1] sowie der erwähnte **BSI-Grundschutz** [12] und speziell dessen Zusatzmodul „IND“ [13] für Industrieumgebungen. Für die weitere Vertiefung werden seitens des BSI zudem Plattformen zum Austausch mit anderen Unternehmen im Kontext der IT-Sicherheit angeboten [16] [17].

Weiterführende Literatur und Informationsquellen

Verbände	Quelle*	Geschäftsleitung	Produktion	IT-Abteilung
[1] **Leitfaden Industrie 4.0 Security,** ISBN 978-3-8163-0689-4 (2016) Inhalt: Handlungsempfehlungen für den Mittelstand, Einführung in das Thema für das ganze Unternehmen (Dokument ist auf Anfrage erhältlich)	VDMA	●	●	●
[2] **Leitfaden Cyber-Sicherheits-Check (2020)** Inhalt: Einführung in eine Analyse der eigenen IT-Sicherheit, Schwerpunkt Office-IT	ZVEI, VDMA, IDSA	○		●
[3] **Fragebogen zur Selbsteinschätzung der IT-Sicherheit (2014)** Inhalt: Hilfestellung zur Selbsteinschätzung im eigenen Unternehmen	VDMA	●	●	●

Bundesstellen	Quelle*	Geschäftsleitung	Produktion	IT-Abteilung
[4] **Sicherheit für die Industrie 4.0, Studie (2016)** Inhalt: Umfangreiche Studie zum Thema IT-Sicherheit in der Industrie	BMWi	●	○	●
[5] **Empfehlungen für Betreiber von ICS – Erfahrungen aus der industriellen Sicherheitsberatung v2.0 (2018)** Inhalt: Kurze Informationsschrift zu den organisatorischen Rahmenbedingungen	BSI	●	●	●
[6] **Empfehlungen für Betreiber von ICS – Fernwartung im industriellen Umfeld v2.0 (2018)** Inhalt: Empfehlungen zum Thema Remote-Service	BSI		○	●
[7] **Empfehlungen für Betreiber von ICS – Industrial Control System Security: Top 10 Bedrohungen (2019)** Inhalt: Zusammenfassung zur IT-Sicherheit, speziell für die Automatisierungstechnik und industrielle Produktion	BSI	●	●	●
[8] **Empfehlungen für Betreiber von ICS – Innentäter v2.0 (2018)** Inhalt: Maßnahmenkatalog und Handlungsempfehlungen	BSI	○		●
[9] **Empfehlungen für Betreiber von ICS – Monitoring und Anomalieerkennung in Produktionsnetzwerken (2019)** Inhalt: Informationsschrift	BSI			●
[10] **Empfehlung zur Cyber-Sicherheit – Sicherheit von Geräten im Internet der Dinge (IoT) (2017)** Inhalt: Handlungsempfehlungen	BSI	○	○	●
[11] **Allgemeine Empfehlungen – Empfehlungen für Fortbildungs- und Qualifizierungsmaßnahmen im ICS-Umfeld (2018)** Inhalt: Handlungsempfehlungen	BSI	●		
[12] **Basis-Absicherung nach IT-Grundschutz (2017)** Inhalt: Empfehlungen zum Umgang mit IT-Sicherheit für das gesamte Unternehmen	BSI	●		●
[13] **Zusatzmodul „IND“ zum IT-Grundschutz (2020)** Inhalt: Besondere Belange von IT-Systemen in der Produktion (ICS, OT)	BSI		●	●

Geschäftsleitung · Produktion · IT-Abteilung · ● voll zuständig · ○ teilweise zuständig

	Wissenschaft und Forschung	Quelle*			
[14]	**Cyberangriffe gegen Unternehmen in Deutschland, Forschungsbericht (2020)** Inhalt: Umfangreiche Studie zur Cyber-Kriminalität, auch als Kurzfassung/Management Summary verfügbar	Kriminol. Forschungs-institut Niedersachsen	●	○	●

	Standardisierung	Quelle*			
[15]	**Normenreihe IEC 62443 (2020)** Inhalt: Mehrteilige internationale Normenreihe zur IT-Sicherheit	IEC			●

	Online-Ressourcen	Quelle*			
[16]	**www.allianz-fuer-cybersicherheit.de** Inhalt: Austauschangebot zur IT-Sicherheit für KMU	BSI	●		●
[17]	**www.it-sicherheit-in-der-wirtschaft.de** Inhalt: Informationsportal zum Thema „IT-Sicherheit“ mit Fokus auf KMU	BSI	●		●
[18]	**Online-Kurs „IT-Grundschutz“** Inhalt: Online-Kurs zur entsprechenden Veröffentlichung	BSI			●

* Die Quellen können über eine einfache Internetrecherche gefunden werden.

Herausgeber
Verein Deutscher Werkzeugmaschinenfabriken e.V. (VDW)
Fachverband Werkzeugmaschinen und
Fertigungssysteme im VDMA
Lyoner Straße 14
60528 Frankfurt am Main
Tel. +49 69 756081-0
Fax +49 69 756081-11
E-Mail vdw@vdw.de
Internet www.vdw.de
Twitter www.twitter.com/VDWonline
YouTube www.youtube.com/metaltradefair

Vorsitzender
Dr. Heinz-Jürgen Prokop,
Trumpf Werkzeugmaschinen GmbH + Co. KG, Ditzingen

Geschäftsführer
Dr. Wilfried Schäfer

Autoren
Arbeitskreis „Steuerungs- und Systemtechnik“ des VDW-Forschungsinstituts, unter fachlicher Beratung von Prof. Dr. Felix Hackelöer, Institut für Automation und Industrial IT (AIT), TH Köln.

Gestaltung
Klaus Bietz \ visuelle Kommunikation, Frankfurt am Main

Druck
h. reuffurth, Mühlheim am Main

Stand
11/2020

Bildnachweis
Adobe Stock

Verein Deutscher Werkzeugmaschinenfabriken e.V. (VDW)
www.vdw.de