Mittelstand 4.0
Kompetenzzentrum
Chemnitz

Betrieb 4.0
machen!

Sicher
Bleiben!

Nachgelesen

Cybersicherheit im digitalen Wandel: Mit Strategie zum Ziel

Heiner Winkler

Mittelstand-
Digital

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Die digitale Transformation birgt beträchtliche Potentiale für Unternehmen, stellt diese aber gleichermaßen hinsichtlich der industriellen Cybersicherheit vor wachsende Herausforderungen. Eine an die betrieblichen Prozesse und Infrastrukturen angepasste IT-Sicherheitsstrategie und innovative Verteidigungsmechanismen sind unabdingbar, um sich dauerhaft vor Hackern zu schützen. Im industriellen Umfeld gibt es dabei Besonderheiten, die es bei der Konzeption und Umsetzung von Cybersicherheit zu beachten gilt.

In dieser Ausgabe unserer *Nachgelesen*-Reihe erfahren Sie:

- welche Gründe für die Digitalisierung sprechen und welche Risiken der Cybersicherheit damit einhergehen,
- was maßgebliche Faktoren für eine sinnvolle IT-Sicherheitsstrategie sind,
- wie sich komplexe Netzwerke im industriellen Umfeld durch das Purdue-Referenz-Modell abstrahieren lassen und
- was sich die hinter der „Defense-in-Depth"-Strategie verbirgt.

Chancen und Risiken der Digitalisierung

Meldungen über ausgeklügelte Cyberattacken, komplexe Hacker-Angriffe und Sicherheitslücken, welche zum Teil Millionen Geräte betreffen, sind allgegenwärtig in den Medien. Von Privatpersonen über Unternehmen und öffentlichen Einrichtungen bis hin zu Kritischen Infrastrukturen (KRITIS) und Regierungen. Treffen kann es jeden. Die Motive der Cyberkriminellen sind multilateral: gezielt Daten zerstören, Geld, Informationen und digitale Identitäten stehlen, Betriebsabläufe stören, ganze Wertschöpfungs- und Lieferketten sabotieren, Produkte verändern, von den Betroffenen digitales Schutzgeld erpressen oder die kompromittierte Tech-Infrastruktur und die erbeuteten Daten für illegale Handlungen nutzen – oder schlichtweg aus reinem Vergnügen.

Das aktuelle Bundeslagebild Cybercrime des Bundeskriminalamtes (BKA) offenbart mit mehr als 100.500 Fällen einen neuen Höchstwert krimineller Internetaktivitäten in Deutschland (über 15 Prozent Steigerung im Vergleich zu 2018) und beziffert den entstandenen Schaden auf rund 87,7 Millionen Euro.[1] Aufgrund des großen Dunkelfeldes liegt der geschätzte monetäre Gesamtschaden mit 102,2 Milliarden Euro weitaus höher, wie eine Studie des Digitalverbandes Bitkom aufzeigt.[2] Im Fokus der Angreifer stehen keinesfalls nur

große Konzerne oder KRITIS-Betreiber, sondern auch zunehmend kleine und mittlere Unternehmen (KMU), wie ebenfalls aus der Studie[2] hervorgeht.

Im Zusammenhang mit den wirtschaftlichen Schwierigkeiten, denen die Großzahl der KMU aufgrund der aktuellen Corona-Situation gegenübersteht, können zielgerichtete Cyberattacken und deren Auswirkungen enormen finanziellen Schaden – bis hin zum Ruin – zur Folge haben.

Demgegenüber stieg die Zahl der deutschen Unternehmen, die sich seit Ausbruch der Pandemie mit der Digitalisierung auseinandergesetzt und diese vorangetrieben haben – und so die negativen Auswirkungen der Krise besser kompensieren. Insbesondere in den Bereichen der Technologie, bei Geschäftsprozessen und Mitarbeitern stiegen die Investitionen in Digitalisierungsmaßnahmen.[3] Die Potenziale der digitalen Transformation liegen in diesem Kontext auf der Hand:

- die Wettbewerbsfähigkeit verbessern,
- betriebliche Prozesse und Abläufe vereinfachen,
- die unternehmerischen Freiheiten steigern,
- die Arbeitsfähigkeit sicherstellen und
- besser auf künftige Krisen vorbereitet sein.

Digitale Technologien ermöglichen die nachhaltige Entwicklung in allen Lebensbereichen, fördern Umwelt- und Klimaschutz und können die Grundlage einer ausgeglichenen Work-Life-Balance darstellen.

Die zunehmende Vernetzung (Internet of Things) und fortschreitende Digitalisierung gewinnt immer mehr an Bedeutung. Damit steigt zwangsläufig die Gefahr, selbst Opfer eines Cyberangriffes, sei es durch gefälschte E-Mails (Phishing), Schadsoftware oder Dienstblockaden (Denial-of Service-Attacken), zu werden. Die Internetkriminalität stellt daher eine der größten Herausforderungen der kommenden Jahrzehnte dar. Umso wichtiger ist der Einsatz von neuen Technologien, um den wachsenden Herausforderungen der IT-Sicherheit angemessen zu begegnen. Für Unternehmen bedeutet das, digitale Kommunikationswege im gesamten – meist historisch gewachsenen heterogenen – Firmennetzwerk abzusichern, die technische Infrastruktur und die darin enthaltenen Daten zu schützen sowie Hackerangriffe zeitnah zu erkennen und abzuwehren.

IT-Sicherheitsstrategie als Basis

Unabhängig von der Größe und Ausrichtung der Unternehmung, ist die Konzeption und Umsetzung eines, an die betrieblichen Abläufe und die Gefahrenlage angepassten, regelmäßig aktualisierten IT-Sicherheitskonzepts unumgänglich. Wie in Abbildung 1 dargestellt, sollte dieses organisatorische Schutzmaßnahmen, die Sensibilisierung und Qualifizierung von Personal sowie den Einsatz und die Pflege einer mehrstufigen Security-Infrastruktur umfassen.

Abbildung 1: Aufbau des IT-Sicherheitskonzepts

Zudem ist es sinnvoll, dass dieses IT-Schutzkonzept die Prävention, Risikobewertung und Ermittlung der Schutzbedarfe, Handlungsweisen und Maßnahmen nach einem erkannten Angriff sowie die forensische Analyse im Nachgang beinhaltet und dynamisch auf alle Komponenten der vernetzten Infrastruktur ausgeweitet wird.

Bekanntermaßen befinden sich in Netzwerken der Betriebstechnologie (OT) viele veraltete Software-Installationen, Systeme mit obsoleter und schwachstellenbehafteter Firmware sowie unsichere Kommunikationsprotokolle im Einsatz. Im Zuge der Umsetzung von Industrie 4.0 werden diese – historisch bedingt als Insellösungen und ohne zuverlässige IT-Sicherheitsmechanismen konzipierten – Plattformen der Industriekommunikation mit den höheren Schichten der Automatisierungspyramide (Abbildung 2) verbunden.

Daraus resultieren komplexe Systeme und Bereiche mit verschiedenen Sicherheitsanforderungen und unterschiedlichem Geschäftswert, welche miteinander gekoppelt werden. Diese konvergenten Netzwerkinfrastrukturen lassen sich nur durch die Kombination aus unterschiedlichen

Produkten, Technologien und Methoden zuverlässig absichern. Das setzt de facto eine umfassende Kenntnis über die bestehenden Netz- und Kommunikationsstrukturen, Komponenten und Schnittstellen voraus.

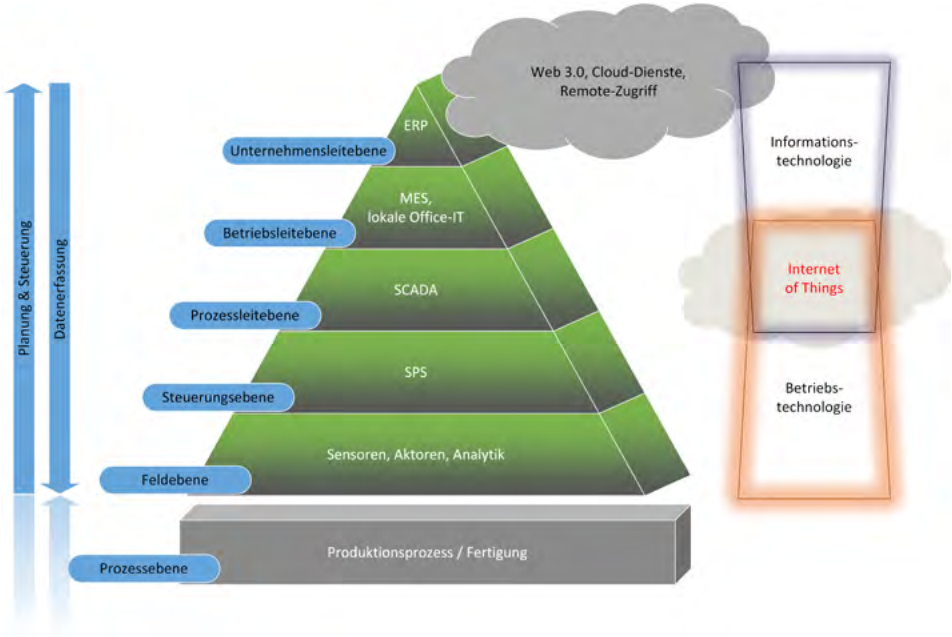

Abbildung 2: Automatisierungspyramide mit konvergenten Netzen

Komplexität reduzieren: Das Purdue-Referenz-Modell

Um in (komplizierten) Industrie-Netzwerken Klarheit und Struktur zu erzeugen, ist es mitunter sinnvoll, diese im ersten Schritt in Form eines Modells zu abstrahieren. Um einen Überblick zu gewinnen und die Vielzahl der heterogenen Komponenten, Protokolle, Prozesse und Schutzbedarfe zu bündeln, kann hier das Purdue-Referenz-Modell sehr hilfreich sein. In diesem Schema wird das gesamte konvergierte Unternehmensnetz in sechs Ebenen, angelehnt an die Stufen der Automatisierungspyramide, untergliedert. Die enthaltenen Systeme und Dienste lassen sich

so dem entsprechenden Level zuordnen. Dies verdeutlicht die schematische Übersicht in Abbildung 3. Eine Besonderheit des Modells ist die Einführung eines Zwischennetzes (Level 4), der demilitarisierten Zone (DMZ). Eine solche DMZ, die sich klassischerweise zwischen unsicherem Internet und IT-Netzwerk befindet, wird hier zur Abgrenzung zwischen OT- und IT-Infrastruktur platziert.4 Darüber lassen sich geteilte Ressourcen zur Verfügung stellen und der sichere Datenaustausch zwischen den konvergierten Netzen realisieren.

Die Abstraktion der Level verfolgt dabei ein zentrales Grundprinzip: Je niedriger die Ebene, umso höher sind die Bedarfe an Verfügbarkeit, Echtzeitfähigkeit und Betriebssicherheit der enthaltenen Netzwerkkomponenten und Prozessabläufe. Daraus ergibt sich der Grundsatz, dass Systeme und Netzbereiche aus einem niedrigeren Level standardmäßig den höheren Leveln nicht vertrauen dürfen.[5] Dieses Paradigma der IT-Sicherheit nennt sich auch Zero-Trust-Modell.

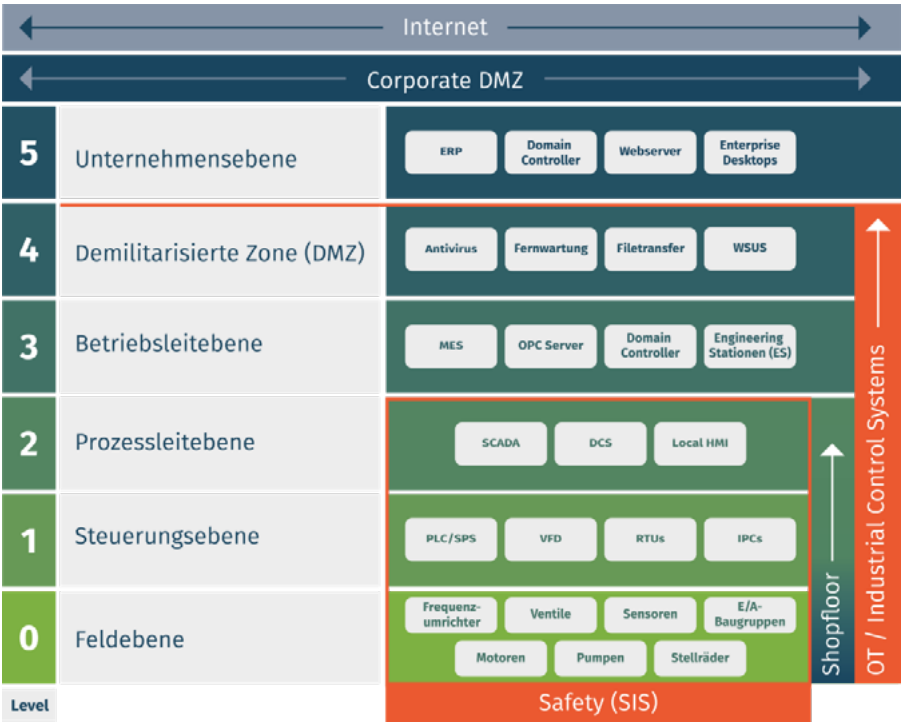

Abbildung 3: Schematische Darstellung des Purdue-Referenz-Modells für industrielle Netze[5]

Sicherheit schaffen: Defense-in-Depth

Auf der Grundlage der Erkenntnisse aus der Anwendung des Purdue-Referenz-Modells lassen sich entsprechende Sicherheitsmaßnahmen umsetzen. So etwa nach dem bewährten Schutzprinzip „Defense-in-Depth“ (DiD), welches der Normenreihe IEC 62443 zu Grunde liegt.[6] Diese internationale Standardserie beschreibt die ganzheitliche Umsetzung von Informationssicherheit im Produktions- und Automatisierungsumfeld. Die aus dem militärischen Bereich kommende DiD-Strategie hat zum Ziel, Angriffserfolge selbst bei Ausschaltung oder Umgehung einzelner Verteidigungslinien unmöglich zu machen. Adaptiert auf die Cybersicherheit für industrielle Netze und Systeme bedeutet das: Mittels aufeinander abgestimmter und sich ergänzender Schutzmaßnahmen, die in mehreren Schichten der Infrastruktur implementiert sind, sollen Cyberattacken auf zu schützende Komponenten, Daten und Dienste erkannt, abgewehrt oder zumindest erheblich erschwert werden. DiD lässt sich auf die gesamte heterogene IT/OT-Infrastruktur eines Unternehmens umsetzen. Vorangestelltes Ziel ist es dabei, sämtliche Vorgänge, Prozessflüsse, Zugriffe, Veränderungen und Anomalien vollständig zu überwachen.

Ein wesentliches Merkmal der Architektur ist die Einführung von Schutzzonen (engl. zones) und Zonenübergängen (engl. conduits). Letztere sind definierte Kommunikationskanäle zwischen den einzelnen Segmenten.

Die Erstellung der einzelnen Segmente kann etwa nach diesen Faktoren erfolgen:

- funktionale Gruppierung (bspw. zusammenhängende Teile einer Anlage)
- gemäß Schutzbedarf (etwa Systeme ohne Update-Versorgung/Virenschutz)
- Überwachungs- und Steuerungselemente (CCTV, SiS, SPS, HMI)
- Zugriff auf Datenbank (-Informationssysteme (bspw. ERP, PDM, MES)
- Systeme für Fernwartung oder Datenaustausch
- nach verwendeten Protokolltypen
- entsprechend der Relevanz für den Geschäftsprozess/betrieblichen Ablauf
- nach Nutzern oder Rollen, Organisationsstrukturen, Zugriffsberechtigungen

Eine nach diesem Prinzip beispielhaft aufgebaute Netzwerkarchitektur eines konvergierten Unternehmensnetzes zeigt Abbildung 4. Wie

darin zu sehen, ist eine horizontale und vertikale Segmentierung in Verbindung mit einem Zero-Trust-Ansatz verwirklicht. Als Kommunikationskanäle zwischen den sechs Netzwerksegmenten sind Zonenübergange definiert. Ein direkter Datenverkehr zwischen OT- und IT-Netz ist per se ausgeschlossen. Wird ein System im Netzwerk von einem Cyberkriminellen kompromittiert, lässt sich der potenzielle Schaden aufgrund des, auf das entsprechende Segment begrenzten Wirkungsgrades, deutlich minimieren.

Bei korrekter Umsetzung schützt die so erschaffene Sicherheitsarchitektur das gesamte Unternehmensnetzwerk nicht nur vor böswilligen Angriffen, sondern kann auch kritischen Kettenreaktionen, welche aus Störungen oder Konfigurationsfehlern einzelner Anlagenbereiche resultieren, zuverlässig vorbeugen.

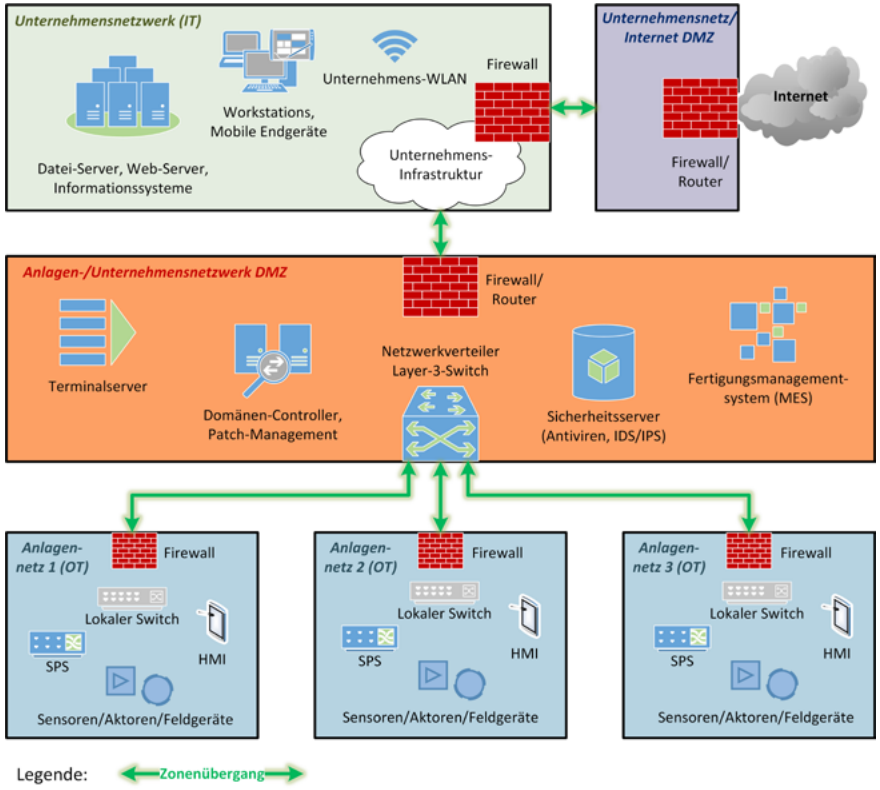

Abbildung 4: Segmentiertes Unternehmensnetzwerk mit definierten Übergängen

Fazit

Um Industrie 4.0 umzusetzen und die Potentiale der digitalen Transformation auszuschöpfen, muss die Konvergenz zwischen klassischer IT und Betriebstechnologie hergestellt werden. Ein solches zukunftsfähiges Netz steigert für Unternehmen zum einen die Chancen, mit Innovationsprojekten auf der bestehenden Netzinfrastruktur aufzusetzen und damit die Wettbewerbsfähigkeit sicherzustellen. Zum anderen entsteht mit der wachsenden Abhängigkeit von digitalen Prozessen ein erhöhter Bedarf an Cybersicherheit. Hierbei empfiehlt sich ein mehrstufiges und der Gefahrenlage angepasstes IT-Sicherheitskonzept.

Die unterschiedlichen Netzwerkanforderungen und Schutzbedarfe sowie die Vielzahl heterogener Systeme bzw. Schnittstellen erfordern ein strukturiertes Vorgehen bei der Planung, Evaluation und Umsetzung von wirksamen Maßnahmen. Um die Robustheit von Netzinfrastrukturen im Umfeld von Industrie 4.0 zu steigern, stellt Defense-in-Depth eine bewährte Strategie dar. Dabei gilt nicht zwangsläufig die Maßgabe, jede einzelne Maschine bzw. jedes (proprietäre) System allumfassend zu schützen. Vielmehr liegt der Fokus darauf, wertvolle Unternehmensdaten und zentrale Prozesse zielgerichtet abzusichern, um so das Risiko und den Wirkungsgrad von unkalkulierbaren Störungen und böswilligen Cyberangriffen zu minimieren.

Anmerkungen

[1] Bundeskriminalamt (BKA) (2019): Cybercrime Bundeslagebild 2019. Abgerufen von: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2019.html [19.02.2021]

[2] Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (2020): Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der vernetzten Welt. Abgerufen von: https://www.bitkom.org/sites/default/files/2020-02/200211_bitkom_studie_wirtschaftsschutz_2020_final.pdf [19.02.2021]

[3] DATEV magazin (2020): Corona treibt Digitalisierung voran – aber nicht alle Unternehmen können mithalten. Abgerufen von: https://www.datev-magazin.de/nachrichten-steuern-recht/wirtschaft/corona-treibt-digitalisierung-voran-aber-nicht-alle-unternehmen-koennen-mithalten-36376 [22.02.2021]

[4] Bundesamt für Sicherheit in der Informationstechnik (BSI) (2013): ICS-Security-Kompendium. Abgerufen von: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf?__blob=publicationFile&v=2 [22.02.2021]

[5] Geiger, M. (2018): Purdue Model: Wie Sie komplizierte Automatisierungs-netze anschaulich überblicken können. Abgerufen von: https://www.sichere-industrie.de/purdue-model-wie-sie-komplizierte-automatisierungsnetze-anschaulich-ueberblicken-koennen/ [22.02.2021]

[6] Kobes, P. (2021): Leitfaden Industrial Security: IEC 62443 einfach erklärt. Vde Verlag GmbH, Berlin

Autor

Heiner Winkler ist wissenschaftlicher Mitarbeiter an der Professur Fabrikplanung und Fabrikbetrieb der Technischen Universität Chemnitz. Im Mittelstand 4.0-Kompetenzzentrum Chemnitz beschäftigt er sich mit den Themen Cybersicherheit, Informationssysteme und Künstliche Intelligenz.

heiner.winkler@betrieb-machen.de

Weitere Informationen

Das Mittelstand 4.0-Kompetenzzentrum Chemnitz gehört zu Mittelstand-Digital. Mit Mittelstand-Digital unterstützt das Bundesministerium für Wirtschaft und Energie die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

Was ist Mittelstand-Digital?
Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Die geförderten Kompetenzzentren helfen mit Expertenwissen, Demonstrationszentren, Best-Practice-Beispielen sowie Netzwerken, die dem Erfahrungsaustausch dienen. Das Bundesministerium für Wirtschaft und Energie (BMWi) ermöglicht die kostenfreie Nutzung aller Angebote von Mittelstand-Digital.

Der DLR Projektträger begleitet im Auftrag des BMWi die Kompetenzzentren fachlich und sorgt für eine bedarfs- und mittelstandsgerechte Umsetzung der Angebote. Das Wissenschaftliche Institut für Infrastruktur und Kommunikationsdienste (WIK) unterstützt mit wissenschaftlicher Begleitung, Vernetzung und Öffentlichkeitsarbeit.

Weitere Informationen finden Sie unter www.mittelstand-digital.de

IMPRESSUM:

Herausgeber:
Mittelstand 4.0-Kompetenzzentrum Chemnitz
Geschäftsstelle
c/o Technische Universität Chemnitz
Prof. Dr.-Ing. habil. Ralph Riedel
DE – 09107 Chemnitz
Tel: 0371 531 19935
Fax: 0371 531 819935
E-Mail: info@betrieb-machen.de
Web: www.betrieb-machen.de
www.kompetenzzentrum-chemnitz.digital

Redaktion & Gestaltung
Heiner Winkler & Anikó Lessi

Bildnachweis Titel:
© Designed by rawpixel.com / Freepik