MSA
The Safety Company

Sichere Vernetzung für Gasdetektionsprogramme ist Realität

Was das für Sicherheitsbeauftragte bedeutet

WIR WISSEN, WORAUF ES ANKOMMT.

Einleitung

Vernetzung begründet eine neue Ära der Arbeitssicherheit. Aber nicht alle Netze sind gleich aufgebaut.

Dieser Fachbeitrag soll Unternehmen im Umgang mit Bedrohungen ihrer Datensicherheit helfen. Es erklärt:

- Warum sich Sicherheitsteams und Unternehmen im Zusammenhang mit „vernetzten Mitarbeitern“ mit der Cybersicherheit beschäftigen sollten.
- Wie sie Lösungen und Partner finden, mit deren Hilfe sie Ihre Arbeitsschutzdaten in der Cloud sichern und schützen können.
- Was zu tun ist, um die Cybersicherheit bei der Gasdetektion in das jeweilige Sicherheitsprogramm einzubinden.

Wer sollte diesen Fachbeitrag lesen?

Sicherheitsbeauftragte, die ...

- ... auf möglichst sichere Weise ein vernetztes Gasdetektionsprogramm aufbauen möchten.
- ... auf der Suche nach einer vernetzten Gassicherheitslösung sind, die den Anforderungen ihres Unternehmens an die Datensicherheit entspricht.
- ... gegenüber cloudbasierten Lösungen skeptisch sind.

Eine vernetzte Welt

Smartphones, Wohnungen und Arbeitsplätze ... die Welt, in der wir leben, vernetzt sich immer stärker. Studien des Pew Research Centre und von Juniper Research zeigen, dass fast die Hälfte der Weltbevölkerung über das Internet verbunden ist – genauer 49 %. Im Jahr 1999, als das Internet noch in den Kinderschuhen steckte, waren es nur 4 %.

Dieselben Forscher schätzen, dass heute weltweit 8,4 Milliarden vernetzte Geräte im Einsatz sind, und dass es im Jahr 2025 im industriellen Internet der Dinge 36,8 Milliarden Verbindungen geben wird. [1,2]

Kurioses 1

Im Jahr 1999, als erst ein kleiner Prozentsatz der Weltbevölkerung mit dem Internet verbunden war und das Web mit allen verfügbaren Informationen füllte, prägte Kevin Ashton, eine Führungskraft des US-Konzerns Procter & Gamble, den Begriff des „Internets der Dinge“. [1,2]

Wissenswertes 1

Das **Internet der Dinge („IoT“ = „Internet of Things“)** ist definiert als „das Netzwerk von Dingen oder Gegenständen, die über das Internet mit anderen Gegenständen, Geräten und Systemen verbunden sind und Daten austauschen“. Im aufstrebenden Internet der Dinge tummeln sich Millionen und Milliarden vernetzter Geräte, die Daten senden und empfangen und das Leben, die Arbeit und die Sicherheit verbessern.[1, 2]

Das **industrielle Internet der Dinge („IIoT“ = „Industrial Internet of Things“)** ist dasselbe wie das Internet der Dinge, nur im industriellen Umfeld. Es ist ein Netzwerk von Sensoren, Geräten, Instrumenten und Gateways, die es diesen „Dingen“ ermöglichen, untereinander und mit der Cloud zu kommunizieren, um Daten zu erfassen und zu übertragen, Automatisierungs- und Steuerungsaufgaben auszuführen und vieles mehr. [1, 2]

Vernetzte Arbeit

Tragbare Messgeräte sind von zentraler Bedeutung für die Vernetzung und Automatisierung im Bereich der Arbeitssicherheit. Umfassende Lösungen mit vernetzter Hard- und Software verschaffen Sicherheitsteams zentralen Datenzugriff und Überblick über die gesamte Arbeitsstätte. Dies kommt der Wirtschaftlichkeit sowie der Sicherheit der Arbeiter und der Arbeitsplätze zugute.

Vernetzte Arbeit mit MSA

MSA nutzt das Sicherheitsmodell von Amazon Web Services zur Anbindung von Geräten an die Cloud und das Internet der Dinge.

Vernetzung und Arbeitssicherheit: Eine Übersicht

Im Bereich der Arbeitssicherheit sind Gasdetektoren ein interessantes Beispiel für das industrielle Internet der Dinge. Die Sensoren der Gasdetektoren erkennen in der Umgebung vorhandene Gase und warnen über die Cloud-Vernetzung Anwender und Sicherheitsteams vor möglichen Gefahren. Wird die Vernetzung nicht richtig gehandhabt, können die von vernetzten Geräten erzeugten Daten die Unternehmen auf neue, ungewohnte Weise bedrohen.

Die meisten Sicherheitsfachkräfte kennen die Hauptvorteile der Vernetzung, darunter:

1. Sicherheitsprogramme können von technologischen Fortschritten profitieren, insbesondere kann die Technologie eine entscheidende zusätzliche technische Sicherheitsbarriere für Mitarbeiter und Arbeitsstätten schaffen.
2. Die Vernetzung ist der Schlüssel zur Förderung der Eigenverantwortlichkeit, zur Rationalisierung von Abläufen und zur einfacheren Einhaltung von Vorschriften.
3. Die von vernetzten Geräten stammenden Daten sind entscheidend für den Aufbau einer Sicherheitskultur und für die Verbesserung der Sicherheitsergebnisse mithilfe von Softwaredienstleitungen.

Kurioses 2

Der Begriff „Softwaredienstleitung“ oder „SaaS“ = „Software as a Service“ wird oft gleichbedeutend mit Cloud Computing verwendet. Softwaredienstleitungen sind eine bedeutende Form der Softwarebereitstellung.

Wissenswertes 2

Softwaredienstleistungen werden auch als „SaaS“ oder „Software as a Service“ bezeichnet. Es handelt sich um sofort einsatzbereite Anwendungen oder Softwarelösungen, welche die Verbindung zu cloudbasierten Programmen und deren Nutzung über das Internet ermöglichen. E-Mail ist eine häufig genutzte Softwaredienstleitung.[1, 2]

SaaS IIoT (Softwaredienstleitungen für das Internet der Dinge) ist das, was wir bei Safety io tun – wir bieten Lösungen auf der Grundlage von drahtlosen Technologien und fortschrittlichem Cloud Computing, die Menschen und wertvolle Infrastrukturen verbinden und schützen. [1, 2]

Die **IIoT-Cloud** ist die zentrale Infrastruktur, die sowohl die Steuerung von „Dingen“ als auch den Datenfluss ermöglicht.[1, 2]

AWS steht für Amazon Web Services und ist die sicherste Plattform für Cloud-Dienstleistungen. AWS verfügt über modernste Sicherheitsinstrumente und unterstützt die meisten Sicherheitsstandards und Compliance-Zertifizierungen. [1, 2]

Vernetzte Arbeit

Mithilfe der tragbaren ALTAIR io™ 4 Gasmessgeräte und der cloudbasierten MSA Grid Software stellt die MSA Connected Work Platform die Verbindung zwischen Anwendern, Arbeitsplätzen und Arbeitsabläufen her und hilft den Sicherheitsbeauftragten mit umsetzbaren Daten bei der Stärkung von Sicherheit und Wirtschaftlichkeit in den Arbeitsumgebungen.

Warum Cybersicherheit bei der Vernetzung von Gasdetektoren wichtig ist

Ein stärker vernetzter Arbeitsplatz birgt ein neues Risiko – nämlich das Risiko von Cyberangriffen. Vernetzte Sicherheitsprogramme müssen robuste Cybersicherheitsmaßnahmen treffen, um die Daten der vernetzten Mitarbeiter zu schützen.

Cybersicherheit ist dann nicht mehr nur eine Angelegenheit des Informationsbeauftragten oder des IT-Teams.
Sie betrifft auch den Sicherheitsbeauftragten und sein Team. Zwei wichtige Gründe dafür sind:

Vertraulichkeit der Daten: Vernetzte tragbare Gasmessgeräte speichern und verarbeiten vertrauliche Informationen, etwa über den Aufenthaltsort der Anwender.

Cyberangriffe sind eine echte, weitverbreitete Gefahr. Allein in den letzten 10 Jahren wurden 11 Milliarden Datensätze von fast 335 Unternehmen entwendet.[3] Diese Sicherheitsverletzungen legten nicht nur vertrauliche Daten offen, sondern sie kosteten die angegriffenen Unternehmen auch viele Millionen. ***Vernetzte Gasdetektionsprogramme sind gegen solcherlei Schäden nicht immun. Aus diesem Grund muss die Sicherheit der Mitarbeiter auch die Sicherheit ihrer vertraulichen Daten mit einschliessen.***

Nützliches 1: Was ist Datenschutz?

Datenschutz ist die Methodik, Daten so zu erfassen, zu übertragen und zu speichern, dass nur befugte Personen darauf zugreifen können.[1, 2]

Nützliches 2: Was sind persönliche Daten?[4]

Persönliche Daten sind alle Informationen, die sich auf eine bestimmte oder bestimmbare lebende Person beziehen. Zusammengenommen können verschiedene Informationen die eindeutige Bestimmung einer Person ermöglichen.
Beispiele persönlicher Daten sind:

- Vor- und Nachname
- Wohnanschrift
- E-Mail-Adresse wie *Vorname.Nachname@Arbeitgeber.com*
- Personalausweisnummer
- Standortdaten aus den Standorteinstellungen eines Mobiltelefons
- Internet-Protokoll-Adresse (IP)
- Cookies
- Advertising IDs auf einem Telefon zur Nachverfolgung von Werbung
- Informationen von Krankenhäusern und Ärzten

Nützliches 3: Was sind persönliche vertrauliche Daten?[5]

Die folgenden persönlichen Daten gelten als vertraulich und müssen auf besondere Weise verarbeitet werden:

- Persönliche Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen hervorgehen
- Mitgliedschaft in einer Gewerkschaft
- Genetische oder biometrische Daten, die ausschließlich zur Bestimmung einer Person verarbeitet werden
- Gesundheitsdaten
- Daten über das Sexualleben oder die sexuelle Ausrichtung einer Person

Nützliches 4: Warum gilt der Standort als vertrauliche Information?[6]

Der Standort gilt als vertrauliche Information, weil er zur Offenlegung anderer zurechenbarer Informationen führen kann. Zurechenbare Informationen sind alle Informationen, welche direkt oder indirekt die Bestimmung einer Person erlauben. Die Bestimmung einer Person erfordert Daten, welche die Person so beschreiben, dass sie sich von allen anderen Personen unterscheidet und als Individuum erkennbar wird. Dazu gehören Name, Identifikationsnummer, Standortdaten, Online-Kennung oder ein oder mehrere Aspekte der physischen, physiologischen, genetischen, mentalen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person.

Vernetztes Arbeiten bei MSA

Zwar ist jedes Unternehmen selbst für die Einhaltung seiner Datenschutzverpflichtungen gegenüber sich und seinen Mitarbeiter verantwortlich, aber MSA hat bereits bei der Entwicklung seiner Connected Work Platform viele Datenschutzvorschriften berücksichtigt, um unseren Kunden deren Einhaltung zu erleichtern.

1. Die persönlichen Daten der Beschäftigten sind Eigentum des Kunden – nicht von MSA oder Safety io.
2. Kunden können auf Wunsch Datenverarbeitungsverträge abschließen.
3. Die MSA Grid Plattform verfügt über Funktionen, die unseren Kunden möglichst viel Spielraum bei der Benennung von Geräten lassen. Die Kunden können die Geräte nach einzelnen Mitarbeitern benennen (etwa „Gerät von Hans Mustermann“), oder weniger persönliche Namen vergeben.

Datenintegrität: Gerätemesswerte und -daten in Verbindung mit Testergebnissen sind für den Schutz der Beschäftigten entscheidend. Sie müssen vollständig und fehlerfrei sein. Bei der Datenintegrität geht es darum, dass Messwerte und Prüfdaten genau und vollständig in die Cloud übertragen werden, unabhängig davon, wie lange die Daten gespeichert werden oder wie oft die Sicherheitsteams darauf zugreifen.

Für Dokumentationszwecke ist es wichtig, dass keine Daten verloren gehen und keine Fehler auftreten. Noch wichtiger ist, dass die Daten den Sicherheitsbeauftragten die benötigten Einblicke geben. Die Datenintegrität stellt sicher, dass die Sicherheitsbeauftragten verstehen können, was zu einer bestimmten Zeit mit einem bestimmten Mitarbeiter oder Messgerät geschieht oder geschehen ist. Die Datenintegrität gewährleistet auch den Schutz der Daten vor Eingriffen von außerhalb. Sicherungsprozesse und Wiederherstellungssysteme sind unerlässlich, wenn die physische Integrität gefährdet ist.

Die **Cybersicherheit der MSA Connected Work Platform** ist ein wesentlicher Teil unserer Grid-Plattform, den wir äußerst ernst nehmen. Der Ansatz von Safety io zur Cybersicherheit beruht auf drei Säulen:

1. Wir legen Wert auf starke Partnerschaften mit branchenführenden Fachleuten. Safety io arbeitet auf dem Gebiet der Cybersicherheit mit branchenführenden Unternehmen zusammen. Unsere Infrastruktur wurde beispielsweise mithilfe von Amazon Web Services (AWS) aufgebaut, das branchenführende Cybersicherheitsteams beschäftigt und ein Maß an Sicherheit bietet, das mit einer selbst erstellten Infrastruktur nur schwer zu erreichen ist.

2. Wir haben Fachwissen eingebaut. Unser engagiertes Cybersicherheitsteam, zu dem auch ein Sicherheitsspezialist gehört, nimmt aktiv an Entscheidungen zur Gestaltung und an der Architekturplanung teil und sorgt auf diese Weise für eine ständige Risikobewertung und die Beachtung sicherer Gestaltungsgrundsätze.

3. Wir schaffen ein Gefühl der Sicherheit und des Vertrauens. Unser Informationssicherheitsmanagementsystem bietet einen Rahmen, der die Cybersicherheit in jeden Bereich unserer täglichen Arbeit einbindet, von der sicheren Softwareentwicklung bis zum physischen Bürozugang. Unser Informationssicherheitsmanagementsystem wurde von einer akkreditierten externen Stelle als konform mit der ISO-Norm 27001:2013 zertifiziert. Die ISO/IEC 27001:2013 ist eine international anerkannte Norm, die bewährte Praktiken des Informationssicherheitsmangements und des Datenschutzes beschreibt.

Vorschriften und Hinweise zur Verarbeitung und Speicherung vertraulicher Mitarbeiterdaten

Während weltweit Gespräche über Datenschutz und Datensicherheit geführt werden, ergreifen Länder und Regionen unterschiedliche Maßnahmen zum Schutz ihrer Bürger. Es folgt ein Überblick über die wichtigsten Maßnahmen zum Schutz von Mitarbeitern.

Internationale Arbeitsorganisation (IAO)

Die IAO verfügt über einen Verhaltenskodex für den Schutz persönlicher Arbeitnehmerdaten. Er ist als Leitfaden für Unternehmen gedacht, ist jedoch nicht verbindlich und ersetzt keine nationalen Gesetze, Vorschriften oder andere internationale Arbeitsnormen.[7] Der IAO zufolge sind persönliche Daten „alle Informationen, die sich auf einen bestimmten oder bestimmbaren Arbeitnehmer beziehen".

Datenschutz-Grundverordnung (DSGVO) der EU

Die Datenschutz-Grundverordnung „versucht, ein Gleichgewicht zwischen starkem Schutz für den Einzelnen und ausreichender Flexibilität für die berechtigten Interessen von Unternehmen und der Öffentlichkeit zu finden". Im Rahmen dieses Balanceakts definiert die Datenschutz-Grundverordnung ausführlich, was persönliche Daten sind und was nicht.[8]

- Alle Unternehmen, die persönliche Daten von Personen in der EU erheben, verwenden oder speichern, müssen die Datenschutz- und Sicherheitsanforderungen der Datenschutz-Grundverordnung einhalten oder mit hohen Geldstrafen rechnen[8]
- Die in der Datenschutz-Grundverordnung vorgesehenen Geldstrafen sollen Verstöße durch große oder kleine Unternehmen zu einem teuren Fehler machen
- Jedes Unternehmen, das die Datenschutz-Grundverordnung nicht einhält, haftet unabhängig von seiner Größe in erheblichem Umfang[9]
- Die Datenschutz-Grundverordnung macht die Wichtigkeit von Datensicherheit und Datenschutz gemäß den Grundsätzen der Datenschutz-Grundverordnung deutlich[10]

Vereinigte Staaten (US)

In den USA regelt kein Bundesgesetz und keine Verfassungsbestimmung die Erhebung und Verwendung persönlicher Daten umfassend.
In jüngster Zeit übernimmt jedoch der Federal Trade Commission Act (FTC Act) die Rolle eines maßgeblichen Gesetzes für den Datenschutz und die Datensicherheit.
Die FTC setzt Richtlinien, wo die Verfassung private Akteure nicht am Missbrauch persönlicher Daten hindert. Sie setzt auch das nationale Verbot unlauterer und betrügerischer Datenschutzpraktiken durch.

Einzelne Bundesstaaten haben umfassendere Datenschutzgesetze mit Anleihen aus mehreren Quellen erlassen, darunter die Datenschutz-Grundverordnung der EU. Ein Beispiel dafür ist der California Consumer Privacy Act (CCPA) (11), der vom Staat Kalifornien erlassen wurde.

Die Sicherheit und Verfügbarkeit von Daten ist nicht nur eine Frage der Einhaltung der Dokumentationsnormen der US-Arbeitsschutzbehörde OSHA und internationaler Vorschriften, sondern auch der Kontrolle über sensible, vertrauliche und geschützte Informationen.

Robuste Cybersicherheitsmaßnahmen sind unerlässlich, um sicherheitsbewusste Unternehmen und ihre Mitarbeiter vor Beeinträchtigungen und Schäden durch Cyberhacker zu schützen.

Worauf Sie bei einer sicheren, cloudbasierten Lösung achten sollten

Sicherheitsbeauftragte, welche die Vorteile eines vernetzten Gasdetektionsprogramms nutzen möchten, müssen sich der Bedeutung der Cybersicherheit bewusst sein und auf eine sichere Vernetzung mithilfe zukunftsweisender Technologien zurückgreifen.

Es gibt sichere Lösungen für ein vernetztes Gasdetektionsprogramm, die den Sicherheitsbeauftragten das Beste aus beiden Welten bieten:

- Verwirklichung von Sicherheitszielen
- Die Gewissheit, dass die Informationen bei der Datenspeicherung und -übertragung geschützt sind

Da der Sicherheitsbeauftragte für die Integrität und Sicherheit seines Gasdetektionsprogramms verantwortlich ist, muss sein Netzwerkpartner nachweisen können, dass die Lösung die strengen, sich ständig ändernden Cybersicherheitsnormen erfüllt und mit ihnen Schritt hält.

Bei der Auswahl eines Netzwerkpartners für eine sichere und vernetzte Lösung sind die folgenden Punkte besonders wichtig:

Umfassende Betriebssicherheit

- Interne, an der Zertifizierungsnorm ISO/IEC 27001:2013 ausgerichtete Richtlinien und Verfahren
- Externe Penetrationstests und Audits
- Interne Schwachstellenanalysen

Sichere Infrastruktur

- Mehrschichtiges Sicherheitsmodell
- Sicheres, hochmodernes Datenhosting (AWS)
- Containerisierung
- Tägliche Tests zur Wiederherstellung von Sicherungskopien
- Die Netzwerktechnik darf nicht zulassen, dass die Hardware für Eingangs-Internetprotokolle wie ICMP erreichbar ist.

Verschlüsselung und Datenschutz

- Bei der Übertragung
- Im Ruhezustand
- Datensicherungen
- Auf Zertifizierungsstandards abgestimmte Richtlinien
- Alle Schnittstellen des Hardware- und Software-Stacks nutzen nur verschlüsselte Protokolle.

Reaktion auf Vorfälle

- Detaillierter Plan zur Reaktion auf Vorfälle
- Umfassende, strenge Tests
- Spezielles Sicherheitsteam

Normen und Zertifizierungen

- ISO 27001:2013
- Datenschutz-Grundverordnung
- Datenschutzrichtlinien im Einklang mit Zertifizierungsnormen

Kultur der Sicherheit

- Hintergrundprüfungen von Mitarbeitern
- Unterzeichnete Vertraulichkeitsvereinbarungen
- Sicherheits- und Datenschutzschulungen für Mitarbeiter
- Sichere Entwicklungspraktiken
- Laptop-Überwachung und Endgeräteschutz
- Netzwerksicherheit und physische Sicherheitsmaßnahmen

Schutz und Kontrollen

- Authentifizierung / Berechtigung
- Endgeräteschutz
- Schutz vor Malware

Die MSA Connected Work Platform deckt alle Bereiche ab, von Zugangskontrollen, Authentifizierung, Verschlüsselung und sicherer Softwareentwicklung bis hin zur Zertifizierung nach der Norm ISO/IEC 27001:2013.

Alle Hardware- und Softwareschnittstellen und Datenübertragungen nutzen verschlüsselte Protokolle. Aufgrund der Beschaffenheit des Netzes sind die MSA-Geräte nicht für Eingangs-Internetprotokolle erreichbar, auch nicht für ICMP. Eine Auflistung der Geräte mittels ICMP ist technisch nicht möglich.

Erfahren Sie mehr darüber, wie MSA und Safety io Ihre Daten schützen.

Hier finden Sie rechtliche Hinweise und Datenschutzerklärung von Safety io.

Umstellung auf eine vernetzte Lösung

Bei MSA bekommen Sie alles. MSA ist führend darin, Sicherheitsbeauftragten zu Gewissheit statt Zweifeln und zu Gelassenheit statt Sorgen und Befürchtungen zu verhelfen. Dazu dient auch seine neu auf dem Markt erschienene vernetzte Sicherheitsplattform, unterstützt von der jüngsten MSA-Produktneuheit: dem tragbaren ALTAIR io™ 4 Gasmessgerät.

Jedes ALTAIR io 4 wird mit der Grid-Software geliefert und ist sofort vernetzt und einsatzbereit. Diese Integration verschafft einen Überblick über die Mitarbeiter, ermöglicht digitale Gerätezuweisung, rationalisiert die Verfahren und veranlasst die Mitarbeiter zu stärkerer Eigenverantwortlichkeit.

Mit einem starken Cybersicherheitsprogramm und von Safety io unterstützter Vernetzung bietet MSA robuste, sichere, durchgängige Gasdetektionslösungen.

Wir möchten Sicherheitsbeauftragten wie Ihnen weiterhelfen, egal an welcher Stelle auf dem Weg zu einer vernetzten Lösung Sie sich befinden.

Verwandeln Sie Ihr Gasdetektionsprogramm in eine mächtige, straffe Sicherheitsplattform.

Unternehmen auf der ganzen Welt nutzen die MSA Grid-Dienste, um ihren Überblick zu schärfen, die Nutzungszeit der Sicherheitsausrüstung zu maximieren, die Eigenverantwortlichkeit der Mitarbeiter zu stärken und Sicherheitsmaßnahmen zu rationalisieren. **Klicken Sie hier und erfahren Sie mehr darüber, was MSA für Sie leisten kann!**

Referenzen

1. https://www.pewresearch.org/internet/2017/06/06/the-internet-of-things-connectivity-binge-what-are-the-implications/
2. https://www.juniperresearch.com/researchstore/devices-technology/industrial-iot-market-research
3. https://www.bloomberg.com/graphics/corporate-hacks-cyber-attacks/index.html
4. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en
5. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en
6. Handbook on European Data Protection Law (Handbuch zum europäischen Datenschutzrecht)
7. https://www.ilo.org/global/topics/safety-and-health-at-work/normative-instruments/code-of-practice/WCMS_107797/lang--en/index.htm
7. https://gdpr.eu/eu-gdpr-personal-data/
7. https://gdpr.eu/fines/
7. https://gdpr.eu/checklist/
7. https://fas.org/sgp/crs/misc/R45631.pdf

Safety io nimmt die Cybersicherheit ernst, aber keine Plattform ist perfekt. Safety io übernimmt keine Garantie dafür, dass die Plattform fehlerfrei funktioniert oder frei von schädlichem Code ist, und die Haftung von Safety io ist gemäß den Nutzungsbedingungen und der SaaS-Vereinbarung beschränkt.

MSA ist weltweit in über vierzig Ländern tätig. Eine MSA Niederlassung in Ihrer Nähe finden Sie unter ***MSAsafety.com/offices***.

1708-002-MC / 09.2022