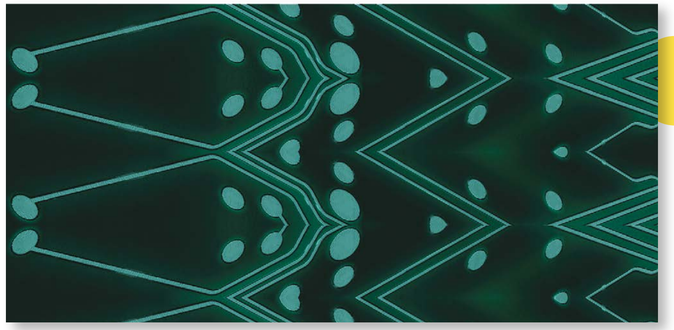
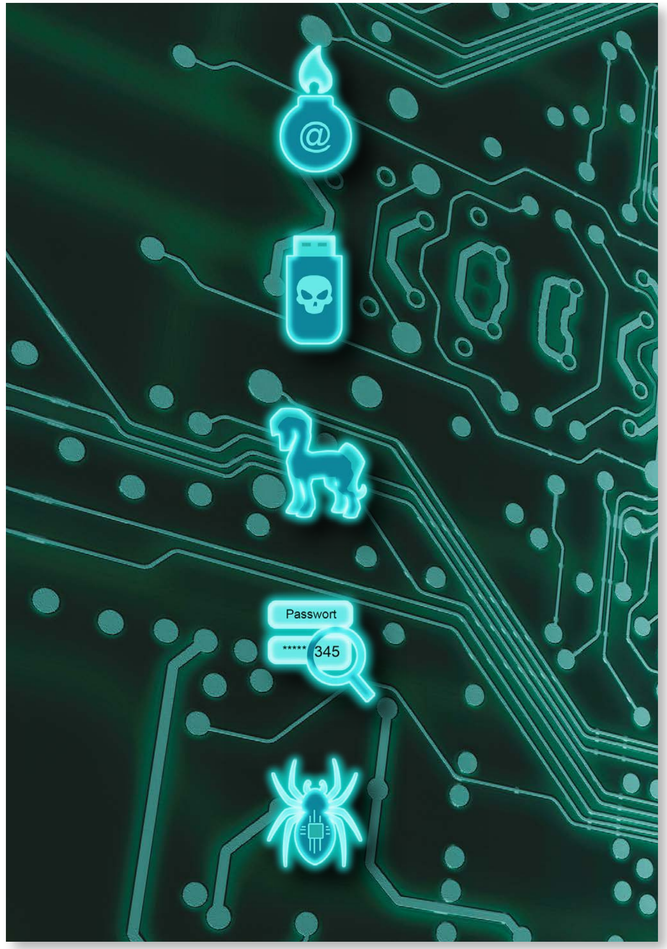


„Zukunft gemeinsam sichern“

V·S·M·A

Ihr Versicherungsmakler für den Maschinen- und Anlagenbau



IT-SICHERHEIT OPTIMIEREN – CYBERRISIKEN MINIMIEREN

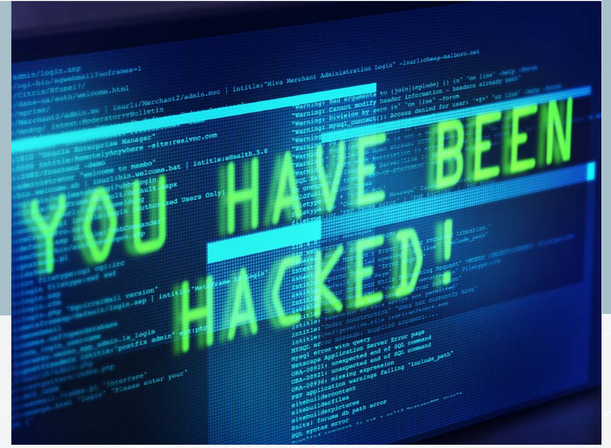
E-Book: Cyber-Tipps für den Maschinen- und Anlagenbau

INHALTSVERZEICHNIS

NUTZUNGSHINWEISE

Um Ihnen die Nutzung des E-Books zu erleichtern, haben wir eine seitliche Navigation integriert. Dort können Sie per Klick zwischen den Kapiteln navigieren – Sie gelangen dann in den Einleitungsbereich des Kapitels. Um einzelne Unterseiten direkt aufzurufen, nutzen Sie bitte das Inhaltsverzeichnis oben. Dort lässt sich jede Seite einzeln auswählen.

VORWORT: JÜRGEN SEIRING, GESCHÄFTSFÜHRER VSMA GMBH



EIN WORT VORAB

Sehr geehrte Damen und Herren,

wussten Sie, dass bereits rund 70 % der deutschen Maschinen- und Anlagenbauer Opfer von Sabotage, Spionage oder Datendiebstahl geworden sind? Eine erstaunlich hohe Zahl!

Dies dürfte damit zusammenhängen, dass viele Unternehmen des Maschinen- und Anlagenbaus auch in den digitalen Welten Innovations- und Marktführer sind. Die intelligent vernetzte Produktion, die mit Industrie 4.0 einhergeht, und innovative Services wie Condition Monitoring und Predictive Maintenance schaffen neue Angriffsflächen für Hacker. Die Digitalisierung steigert zwar die Effizienz – aber eben auch die Zahl der Cyberangriffe.

Sicher ist: Der Schutz von Daten und Know-how ist im Maschinen- und Anlagenbau wichtiger denn je. Daher haben wir gemeinsam mit dem VDMA die Initiative „Unternehmen Cybersicherheit" ins Leben gerufen, die Sie im Kampf gegen Cyberkriminelle unterstützen möchte. Das vorliegende E-Book ist ein Teil dieses Angebots. Auf den folgenden Seiten erwarten Sie neben aktuellen Infos zur Cyberrisiko-Lage in Deutschland auch praxisorientierte Tipps, Checklisten und Arbeitshilfen, die Sie direkt vom E-Book aus bestellen können.

Ich wünsche Ihnen eine inspirierende Lektüre und stehe Ihnen für Fragen gerne zur Verfügung.

Jürgen Seiring

„DIGITALE GESCHÄFTSMODELLE ERHÖHEN DIE ANGRIFFSFLÄCHE“

Sehr geehrter Herr Brodtmann (Hauptgeschäftsführer des VDMA e. V.), Sie beschäftigen sich täglich mit neuen Risiken für die Branche, wie z. B. der wachsenden Gefahr, die von Cyberkriminellen ausgeht. Warum ist der Maschinen- und Anlagenbau Ihrer Meinung nach ein besonders beliebtes Ziel?

Cyber-Risiken nehmen im Maschinen- und Anlagenbau in dem Maße zu, in dem die Digitalisierung in unserer Branche Platz greift. Intelligente Produkte, intelligente Prozesse und letztlich auch digitale Geschäftsmodelle bieten eine größere Angriffsfläche für Cyberkriminelle, als das in der Vergangenheit der Fall war.

Gibt es weitere Gründe, die die VDMA-Mitgliedsunternehmen für Hacker attraktiv machen?
Definitiv! Wir haben eine Menge von „Hidden Champions“ in unserer Branche, an deren Know-how auch viele andere interessiert sind. Und am Ende werden digitale Geschäftsmodelle eine Verlängerung des Services mit sich bringen – Predictive Maintenance und andere Dinge –, sodass die Angriffsfläche noch weiter erhöht wird.

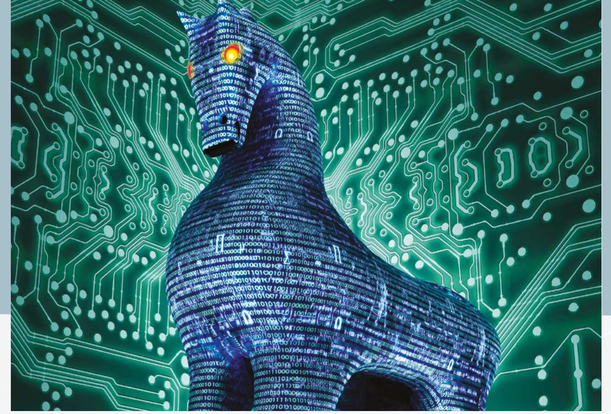
Sind den Mitgliedsunternehmen diese Risiken bewusst?
Cyber-Risiken werden im Maschinenbau und in unseren Mitgliedsunternehmen noch unterschätzt. Das zeigt auch eine Studie, die wir gemeinsam mit unserem Tochterunternehmen, der VSMA GmbH, erstellt haben. Die Studie ist für Mitglieder gratis und kann hier bestellt werden.

Zu welchen Ergebnissen kommt diese Studie?
Die Cyber-Studie zeigt, dass das gesamte Thema der Cyber-Risiken noch nicht flächendeckend in der Geschäftsführungsebene angekommen ist und bei 88 % der Unternehmen noch kein hinreichender Schutz besteht. Das hat natürlich auch damit zu tun, dass es bisher wenig passende Angebote an Cyber-Versicherungen gegeben hat.

Wie hat der VDMA auf die beunruhigenden Ergebnisse der Cyber-Studie reagiert?
Um unsere Mitgliedsunternehmen dabei zu unterstützen, sich besser gegen Cyberangriffe abzusichern, haben wir gemeinsam mit unserer Tochtergesellschaft, der VSMA GmbH, eine maßgeschneiderte Versicherungslösung entwickelt, die die bisherige Deckungslücke schließen kann – die VDMA Cyber-Police™.

JETZT STUDIE BESTELLEN

Inhaltsverzeichnis
Einleitung
Cyber-Risiken & IT-Sicherheit
Ransomware & Phishing
IT-Sicherheit im Home-Office
VDMA Cyber-Police (VCP)
VCP-Angebot anfragen
Cyber-Newsletter abonnieren

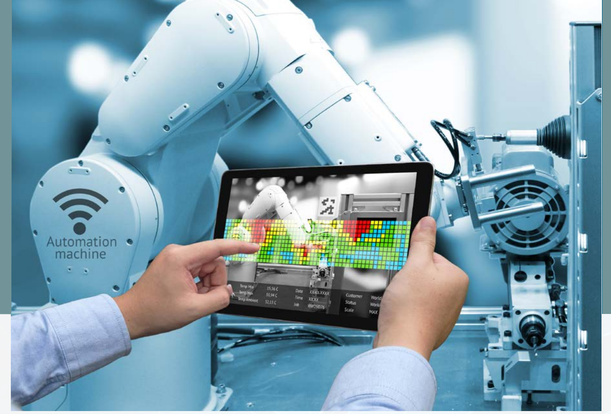


CYBER-RISIKEN IM MASCHINEN- UND ANLAGENBAU

CYBER-VIDEO: SO HALTEN SIE IHRE CYBER-RISIKEN IM ZAUM

Phishing, Viren und Trojaner – Cyberangriffe sind heutzutage an der Tagesordnung und verursachen Schäden in Milliardenhöhe. Auch der Maschinen- und Anlagenbau wird immer häufiger zum Ziel. Warum das so ist und wie Sie sich absichern, erfahren Sie hier:

Inhaltsverzeichnis
Einleitung
Cyber-Risiken & IT-Sicherheit
Ransomware & Phishing
IT-Sicherheit im Home-Office
VDMA Cyber-Police (VCP)
VCP-Angebot anfragen
Cyber-Newsletter abonnieren

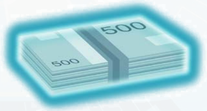


EINLEITUNG

HACKERANGRIFFE SIND DIE GRÖSSTE BEDROHUNG DES 21. JAHRHUNDERTS

Der Maschinen- und Anlagenbau ist in vielen Bereichen Weltmarktführer – und damit besonders interessant für Kriminelle. In der Digitalisierung und Automatisierung ist die Branche extrem fortschrittlich. Das macht sie besonders anfällig für Hackerangriffe. Der Verfassungsschutz registriert alle drei Minuten einen Angriff auf eine deutsche Firma. Im Ernstfall ist der Schaden groß, Summen in sechsstelliger Höhe sind keine Seltenheit.

70 % DER INDUSTRIEUNTERNEHMEN
in Deutschland hatten bereits
einen Cybervorfall.



50 MILLIARDEN € SCHADEN PRO JAHR
verursachen Cyberangriffe
auf deutsche Unternehmen.

59 % DER CYBERANGRIFFE
führen zu Betriebsunterbrechungen
und Produktionsausfällen.

Inhaltsverzeichnis
Einleitung
Cyber-Risiken & IT-Sicherheit
Ransomware & Phishing
IT-Sicherheit im Home-Office
VDMA Cyber-Police (VCP)
VCP-Angebot anfragen
Cyber-Newsletter abonnieren

IT-NOTFALLPLAN UND IT-NOTFALLKARTE

ARBEITSHILFEN ZUR VORBEREITUNG AUF DEN ERNSTFALL

DER MUSTER IT-NOTFALLPLAN

Wenn wichtige IT-Systeme beeinträchtigt sind, ist Eile geboten. Jedes Unternehmen sollte daher über einen IT-Notfallplan verfügen, der das interne Vorgehen regelt.

Der Muster IT-Notfallplan enthält Vorschläge zum Umgang mit Cybervorfällen – vom Notbetrieb über Sofortmaßnahmen bis zur Wiederaufnahme des Betriebs. Die Vorlage ist für VDMA-Mitglieder kostenlos.

JETZT NOTFALLPLAN BESTELLEN

DIE MUSTER IT-NOTFALLKARTE

Viele Mitarbeiter wissen im Ernstfall nicht, wie sie reagieren sollen. Eine echte Hilfestellung ist eine IT-Notfallkarte, die Ihre Mitarbeiter schnell mit wichtigen Verhaltensregeln unterstützt.

Die IT-Notfallkarte sollte jedem Home-Office-Mitarbeiter ausgehändigt und im Unternehmen selbst an gut sichtbarer Stelle aufgehängt werden. Das Muster ist für VDMA-Mitgliedsunternehmen gratis.

JETZT NOTFALLKARTE BESTELLEN

Inhaltsverzeichnis

Einleitung

Cyber-Risiken & IT-Sicherheit

Ransomware & Phishing

IT-Sicherheit im Home-Office

VDMA Cyber-Police (VCP)

VCP-Angebot anfragen

Cyber-Newsletter abonnieren

CHECKLISTE: VERHALTENSREGELN IM ERNSTFALL

RICHTIG REAGIEREN: BEI CYBERVORFÄLLEN IST UMSICHT GEBOTEN

- **Verändern Sie das System nicht**
  Durch einen vorschnellen Neustart können Spuren im Arbeitsspeicher vernichtet werden. Schalten Sie das System nur ab, wenn Ihr IT-Experte zu dieser Maßnahme rät.
- **Krisenstab/Notfallteam**
  Informieren Sie unverzüglich alle Mitglieder Ihres Cyber-Notfallteams und stellen Sie alle Beteiligten bis zur Bewältigung und Aufklärung des Cyberangriffs von weiteren Aufgaben frei.
- **Umfassende Anfangsanalyse**
  Zunächst muss ein IT-Forensiker genau prüfen, welche Systeme von dem Angriff tatsächlich betroffen sind. Cyberkriminelle spiegeln oft unwahre Sachverhalte vor, um ihre Ziele zu erreichen.
- **Beweismittel forensisch sichern**
  Um eine lückenlose Untersuchung des Vorfalls zu ermöglichen, sollten Sie den Zugang zu allen Beweismitteln einschränken, bis diese durch einen IT-Forensiker ge-sichert wurden.
- **Dokumentation des Vorgehens**
  Protokollieren Sie genau, wer Zugriff auf welche Systeme und Beweismittel hatte, und halten Sie die örtlichen Gegebenheiten und eventuelle Bildschirmansichten fotografisch fest.
- **Forensik-Experten einschalten**
  Falls Sie keine eigenen IT-Forensiker beschäftigen, ziehen Sie unbedingt externe Fachleute hinzu, die den gesamten Vorfall gerichtsfest aufklären und aufarbeiten können.
- **Sachverhalt dokumentieren**
  Ermitteln Sie die genaue Art, den Umfang, das Ausmaß und den zeitlichen Verlauf der Cyberattacke und halten Sie alle Erkenntnisse und ergriffenen Maßnahmen akribisch fest.
- **Meldepflichten beachten**
  Jeder Cyberangriff, bei dem personenbezogene Daten in die Hände von unberechtigten Dritten gelangt sind, ist meldepflichtig! Informieren Sie unverzüglich die zuständige Aufsichtsbehörde.
- **Sicherheitsvorkehrungen optimieren**
  Oft folgen auf den ersten Angriff sofort weitere. Erhöhen Sie daher umgehend Ihre Sicherheit und führen Sie Penetrationstests durch, um Schwachstellen aufzudecken.
- **Täter-Profiling**
  Eine genaue Analyse der Angriffsziele und Absichten der Täter bringt wichtige Erkenntnisse, mit denen sich weitere Attacken in Zukunft eventuell verhindern lassen.

Inhaltsverzeichnis
Einleitung
Cyber-Risiken & IT-Sicherheit
Ransomware & Phishing
IT-Sicherheit im Home-Office
VDMA Cyber-Police (VCP)
VCP-Angebot anfragen
Cyber-Newsletter abonnieren

RECHTZEITIG VORBEUGEN: FÜNF TIPPS ZUR IT-SICHERHEIT IN DER PRODUKTION

TIPP 1:

IT-Sicherheit ist Chefsache

Diesbezüglich sind sich die VDMA-Experten einig: Die finale Zuständigkeit für das Thema IT-Sicherheit muss bei einem Mitglied der Geschäftsführung oder des Vorstandes liegen. Sonst fehlt es dem IT-Verantwortlichen im Ernstfall an der erforderlichen Rückendeckung. IT-Sicherheitsziele und Verantwortlichkeiten müssen zudem klar und eindeutig in einem Sicherheitskonzept festgelegt werden – das gilt sowohl für den Office- als auch für den Produktionsbereich. Wichtig: Das Konzept muss regelmäßig aktualisiert werden.

TIPP 2:

Notfallmanagement implementieren

Ein durchdachtes IT-Notfallmanagement ist unverzichtbar, um zeitnah und koordiniert auf Störfälle reagieren zu können. Dafür benötigen Sie einen Notfallplan, der personelle Zuständigkeiten sowie technische, organisatorische und juristische Maßnahmen exakt festgelegt. Falls Sie über keinen Notfallplan verfügen, finden Sie hier ein Muster. Weitere Infos und Muster zum Thema Notfallmanagement finden Sie auf der Webseite des Bundesamts für Sicherheit in der Informationstechnik (BSI) (www.bsi.bund.de).

TIPP 3:

Technische Schutzmaßnahmen i. d. Produktion

In einer Produktionsumgebung sind effiziente technische Schutzmaßnahmen besonders bedeutsam. Zur Absicherung der Maschinen und Anlagen sollten Sie bestenfalls das gesamte Netzwerk der Produktions-IT in separate Sicherheitszellen unterteilen und diese jeweils gesondert mit einer Firewall schützen. Eine durchdachte Netzwerktrennung bzw. -segmentierung verhindert, dass im Störfall die ganze Produktion betroffen ist. Im günstigsten Fall ist jede Maschine bzw. Anlage durch eine eigene Firewall gesichert.

TIPP 4:

Zugangsschutz und Mitarbeitersensibilisierung

In Sachen Zugangsschutz sollten Sie sich stets die Frage stellen, ob alle Anwender auch nur und ausschließlich die Rechte haben, die sie benötigen. Immer noch werden die meisten IT-Sicherheitsvorfälle durch Mitarbeiter verursacht. Achten Sie auf ein gutes Berechtigungs- und Passwortmanagement und sichern Sie alle Zugänge bzw. Schnittstellen (z. B. USB, LAN, WLAN) ab. Regelmäßige Mitarbeiterschulungen zu den Themen IT-Sicherheit, Datenschutz und speziellen Angriffsarten verringern das Cyberrisiko.

TIPP 5:

Fernwartung kontrollieren

Der externe Zugriff auf die Produktions-IT ist ein besonders kritischer Vorgang. Alle Fernwartungszugänge sollten daher technisch und organisatorisch gesichert werden (z. B. Firewall, Anforderungen an Dienstleister). Ein Zugriff sollte außerdem nur über sichere Verbindungen (VPN) und Protokolle (z. B. IPsec, SSH, SSL) erfolgen. Vermeiden Sie den pauschalen Zugriff auf größere Netzbereiche und ermöglichen Sie nur gezielte Zugriffe auf ausgewählte Einzelkomponenten innerhalb von festgelegten Zeitfenstern.

Inhaltsverzeichnis

Einleitung

Cyber-Risiken & IT-Sicherheit

Ransomware & Phishing

IT-Sicherheit im Home-Office

VDMA Cyber-Police (VCP)

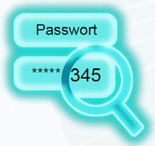
VCP-Angebot anfragen

Cyber-Newsletter abonnieren

EINLEITUNG

PHISHING UND SCHADPROGRAMME SIND DAS GRÖSSTE SICHERHEITSRISIKO

Rund 70 % aller erfolgreichen Hackerangriffe beginnen mit einer E-Mail. Über Nachrichten, die von der Hausbank, von Bewerbern oder sogar von Kollegen oder Kunden zu stammen scheinen, schleusen Hacker Ransomware wie zum Beispiel den gefährlichen Verschlüsselungstrojaner Emotet ein. Ist ein System erstmal infiziert, verbreitet sich der virtuelle Schädling weiter und kann schlimmstenfalls das gesamte IT-System und die Produktion lahmlegen.



46.000 PHISHING-WEBSEITEN
pro Tag werden Studien zufolge von Hackern derzeit im Schnitt generiert – Tendenz steigend.

18 MILLIONEN
Phishing- und Malware-Angriffe mit Coronabezug stoppt allein Google zurzeit täglich.

230.000 COMPUTER
infizierte die Schadsoftware WannaCry im Mai 2017 innerhalb eines einzigen Tages.

Inhaltsverzeichnis
Einleitung
Cyber-Risiken & IT-Sicherheit
Ransomware & Phishing
IT-Sicherheit im Home-Office
VDMA Cyber-Police (VCP)
VCP-Angebot anfragen
Cyber-Newsletter abonnieren

CHECKLISTE: ANZEICHEN FÜR EINEN RANSOMWARE-ANGRIFF

DIESE INDIKATOREN SPRECHEN FÜR EINE RANSOMWARE-ATTACKE

- Rechner wird langsam und reagiert verzögert
- Dateien lassen sich plötzlich nicht mehr öffnen
- Entdeckung verschlüsselter bzw. nicht lesbarer Dateien
- Entdeckung unbekannter Dateien/Dateiendungen
- Plötzliche Neustarts oder Neustart in den abgesicherten Modus
- Anti-Virus-Software deaktiviert/zeigt Fehler und startet nicht
- Aufforderung zur Installation eines Programms
- Aufforderung zur Eingabe des Administrator-Passworts
- Änderung des Desktophintergrunds
- Lösegeld-Bildschirm-Meldung oder Lösegeld-Meldung bei Systemstart
- E-Mails mit ungewöhnlichen oder unerwarteten Anhängen
- E-Mails mit Links oder Aufforderungen, ungewohnte Dinge zu tun

„VDMA NOTFALLHILFE-RANSOMWARE" MIT WERTVOLLEN TIPPS UND INFORMATIONEN

Auch auf Administrator-Ebene gibt es Indikatoren, die für einen Ransomware-Angriff sprechen. Diese finden Sie in der VDMA-Broschüre „Notfallhilfe Ransomware", die vom VDMA Competence Center Industrial Security entwickelt wurde. Das Notfallpapier wurde und ist für Mitgliedsunternehmen kostenlos erhältlich und kann **hier** online angefordert werden.

Inhaltsverzeichnis
Einleitung
Cyber-Risiken & IT-Sicherheit
Ransomware & Phishing
IT-Sicherheit im Home-Office
VDMA Cyber-Police (VCP)
VCP-Angebot anfragen
Cyber-Newsletter abonnieren

TIPPS: PHISHING-RISIKO IM UNTERNEHMEN MINIMIEREN

VORSICHT GEFÄHRLICHE E-MAIL: SO VERRINGERN SIE DAS PHISHING-RISIKO

TIPP 1:

Absicherung des E-Mail-Clients

Ergänzen Sie Ihre E-Mail-Client-Software durch schützende Software-Komponenten, die Sie durch regelmäßige Updates auf dem neuesten Stand halten. Dazu sollten neben einem Virenschutzprogramm und einer effektiven Firewall auch Anti-Spam- und Anti-Phishing-Software gehören.

TIPP 2:

Verschlüsselung und Signatur

Verwenden Sie bei der Anbindung der E-Mail-Clients standardisierte Protokolle, die mittels SSL/TLS (Secure Socket Layer/Transport Layer Security) durch Authentisierung und Verschlüsselung gesichert werden. Führen Sie zusätzlich in Ihren Unternehmen digitale Signaturen ein.

TIPP 3:

Interne E-Mail-Richtlinie

Erstellen Sie eine E-Mail-Richtlinie für Ihre Mitarbeiter mit genauen Anweisungen. Dort können Sie z. B. verbindlich regeln, wie mit E-Mail-Anhängen umzugehen ist, welche Inhalte als „verdächtig" einzuschätzen sind und wer für die Überprüfung fragwürdiger E-Mails zuständig ist.

TIPP 4:

Schulungen und Checklisten

Gezielte Cyber-Angriffe z. B. durch Spear-Phishing sind selbst für vorsichtige Mitarbeiter kaum zu erkennen. Führen Sie jährliche Schulungen zum Thema durch und informieren Sie über aktuelle Angriffsarten. Geben Sie Ihren Mitarbeitern Checklisten zum Umgang mit verdächtigen E-Mails an die Hand.

TIPP 5:

Phishing-Simulation im Unternehmen

Ein gutes Mittel zur Sensibilisierung sind Phishing-Tests. Dabei werden simulierte Phishing-E-Mails mit –harmlosen – Anhängen oder Links verschickt, um Ihre Mitarbeiter zu testen. Das Ergebnis verschafft Ihnen einen Überblick über die Lage und kann zudem zu Schulungszwecken verwendet werden.

Inhaltsverzeichnis
Einleitung
Cyber-Risiken & IT-Sicherheit
Ransomware & Phishing
IT-Sicherheit im Home-Office
VDMA Cyber-Police (VCP)
VCP-Angebot anfragen
Cyber-Newsletter abonnieren

HOME-OFFICE ÖFFNET NEUE EINFALLSTORE FÜR HACKER

Seit Beginn der Coronakrise haben Cyberkriminelle Hochkonjunktur. Ein Grund für den Boom ist die zunehmende Anzahl an Home-Office-Arbeitsplätzen. Private Firewalls sind leichter zu knacken, isolierte Mitarbeiter klicken eher auf gefährliche E-Mail-Anhänge und Videokonferenzen ziehen unerwünschte Gäste an. Die umfassende plötzliche Mehrnutzung von Digitalisierungsprodukten eröffnet Angreifern so insgesamt eine stark vergrößerte Angriffsfläche für ihre kriminellen Aktivitäten.

MEHR HOME-OFFICE-PLÄTZE

49 % der Arbeitnehmer sind derzeit im Home-Office tätig

HACKER FINDEN LEICHTER ZUGANG

Fritzbox statt Firewall: Hacker nutzen neue Einfallstore aus

CYBERANGRIFFE NEHMEN ZU

33 % mehr Hackerangriffe – Tendenz steigend

Inhaltsverzeichnis

Einleitung

Cyber-Risiken & IT-Sicherheit

Ransomware & Phishing

IT-Sicherheit im Home-Office

VDMA Cyber-Police (VCP)

VCP-Angebot anfragen

Cyber-Newsletter abonnieren

TIPPS: ERSTE MASSNAHMEN FÜR EIN CYBERSICHERES HOME-OFFICE

IT-SICHERHEIT IM HOME-OFFICE: DARAUF SOLLTEN UNTERNEHMEN ACHTEN

TIPP 1: Schulung der Home-Office-Mitarbeiter

Wenn es um IT-Sicherheit geht, sollten Sie die „Schwachstelle Mensch" bedenken. Die Distanz zu Kollegen und Firmen-Infrastruktur macht viele Mitarbeiter unvorsichtig. Arbeitnehmer im Home-Office sollten daher regelmäßig geschult und sensibilisiert werden. Informieren Sie über aktuelle Risiken anhand konkreter Fallbeispielen, erlassen Sie klare Richtlinien und planen Sie Schulungen ein.

TIPP 2: Zugriff nur über sichere VPN-Umgebung

Für den Fernzugriff auf das Firmennetzwerk muss ein sicherer Remote-Zugang eingerichtet werden, z. B. ein kryptografisch abgesichertes Virtual Private Network (VPN). Stellen Sie sicher, dass Mitarbeiter nur über diesen Kanal (VPN) auf interne Server/ Netzwerke zugreifen können. Beschränken Sie den Zugriff auf vertrauenswürdige Benutzer bzw. IT-Systeme und notwendige Nutzungszeiten.

TIPP 3: IT-Schutzmaßnahmen im Home-Office

Überprüfen Sie regelmäßig, ob Software und Applikationen auf allen externen Firmengeräten auf dem neuesten Stand sind, und beseitigen Sie Schwachstellen sofort durch entsprechende Software-Patches. Auch klassische Standardmaßnahmen zum Schutz Ihrer externen IT-Systeme sind absolut unverzichtbar. Setzen Sie unbedingt ein geeignetes Antivirenprogramm und eine Firewall ein.

TIPP 4: Tragbare IT-Systeme und Datenträger verschlüsseln

Dienstliche IT-Geräte können während einer Bahnfahrt, aus einem Hotelzimmer oder gar direkt aus dem Home-Office entwendet werden. Hinzu kommt, dass mobile Geräte oftmals nicht so gut abgesichert sind wie der Arbeitsplatz. Tragbare IT-Systeme, Endgeräte und Datenträger sollten daher stets aufwendig verschlüsselt werden, um einen Fremdzugriff auf sensible Firmendaten zu verhindern.

TIPP 5: Auf Multi-Faktor-Authentifizierung umstellen

Führen Sie, wo immer möglich, eine Multi-Faktor-Authentifizierung für Ihre Konten ein. Auf diese Weise müssen mindestens zwei Authentifizierungsfaktoren bzw. Nachweise vorliegen, bevor auf Daten zugegriffen werden kann. Der Zusatzschutz ist vor allem dann wichtig, wenn viele Mitarbeiter von außerhalb auf Netzwerke zugreifen und Angreifer dadurch mehr Zugangspunkte haben.

Inhaltsverzeichnis
Einleitung
Cyber-Risiken & IT-Sicherheit
Ransomware & Phishing
IT-Sicherheit im Home-Office
VDMA Cyber-Police (VCP)
VCP-Angebot anfragen
Cyber-Newsletter abonnieren

CHECKLISTE: ARBEITEN IM HOME-OFFICE

CYBERSICHERES HOME-OFFICE: CHECKLISTE FÜR MITARBEITER

- **Nutzen Sie möglichst nur Firmengeräte**
  Fragen Sie Ihren Arbeitgeber nach sicher konfigurierten Geräten fürs Home-Office. Dazu gehören PC, Smartphone und Zubehör wie z. B. USB-Sticks.

- **Trennen Sie Geschäftliches von Privatem**
  Sobald Sie mit dem Firmennetzwerk verbunden sind, sind alle privaten Anwendungen im Hintergrund zu vermeiden. Dazu gehören auch E-Mails.

- **Zugriff nur über sichere VPN-Verbindung**
  Greifen Sie grundsätzlich nur über ein professionell kryptografisch abgesichertes Virtual Private Network (VPN) auf firmeninterne Netzwerke und Server zu.

- **WLAN-Router vor Zugriff schützen**
  Ändern Sie das Passwort Ihres WLAN-Routers. Das Passwort sollte mindestens 18 Zeichen lang sein. Nutzen Sie für die Erstellung einen Passwort-Generator.

- **Regelmäßige Updates sind Pflicht**
  Aktualisieren Sie laufend Ihren Virenscanner sowie installierte Anwendungen und Software. Fragen Sie im Zweifel bei Ihrer IT-Abteilung nach.

- **Passwortschutz ernst nehmen**
  Verwenden Sie starke Passwörter mit mindestens 12 Zeichen (inkl. Zahlen und Sonderzeichen). Nutzen Sie einen professionellen Passwort-Generator.

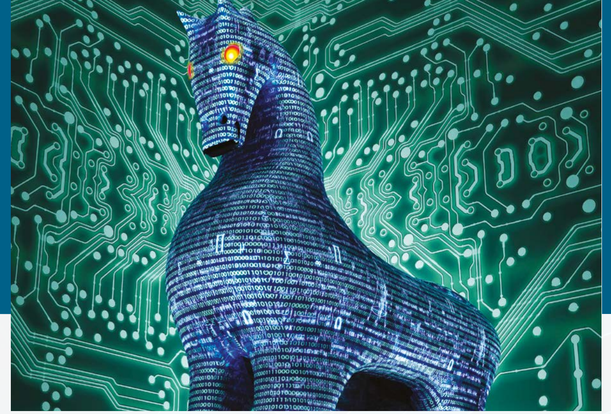
- **Phishing-Mails nehmen stark zu**
  Checken Sie alle E-Mails vor dem Öffnen lieber doppelt! Phishing-Angriffe nehmen aktuell stark zu. Praktische Tipps zum Thema Phishing finden Sie hier.

- **Keine Datenpreisgabe am Telefon**
  Home-Office-Mitarbeiter sind beliebte Ziele für Social-Engineering-Angriffe. Geben Sie am Telefon keine Passwörter, Bankdaten oder persönl. Daten preis.

- **Messenger und Videokonferenz**
  Im Home-Office fehlt der schnelle Austausch mit Kollegen? Nutzen Sie dafür ausschließlich Dienste, die Ihr Arbeitgeber autorisiert und gesichert hat.

- **Datensicherung auf dem Firmenserver**
  Speichern Sie wichtige Dokumente/Daten möglichst direkt auf dem Firmenserver oder übertragen Sie die Daten zumindest in einem regelmäßigen Turnus.

Inhaltsverzeichnis
Einleitung
Cyber-Risiken & IT-Sicherheit
Ransomware & Phishing
IT-Sicherheit im Home-Office
VDMA Cyber-Police (VCP)
VCP-Angebot anfragen
Cyber-Newsletter abonnieren



DIE CYBER-VERSICHERUNG FÜR DEN MASCHINEN- UND ANLAGENBAU

Die Zahl der Attacken auf VDMA-Mitgliedsunternehmen wächst unaufhörlich. Eine Kurzumfrage des VDMA ergab, dass in den letzten beiden Jahren rund 40 % der Unternehmen „erfolgreich" via Social Engineering und Phishing angegriffen wurden – bei 34 % wurde zudem Schadsoftware in die Produktion eingeschleust. Die Folge: IT- und Produktionsausfälle, die Schäden in Millionenhöhe verursachten. Daher hat der VDMA gemeinsam mit der VSMA GmbH eine auf die Anforderungen der Branche ausgerichtete Versicherungslösung entwickelt, die umfassenden Deckungsschutz bietet.

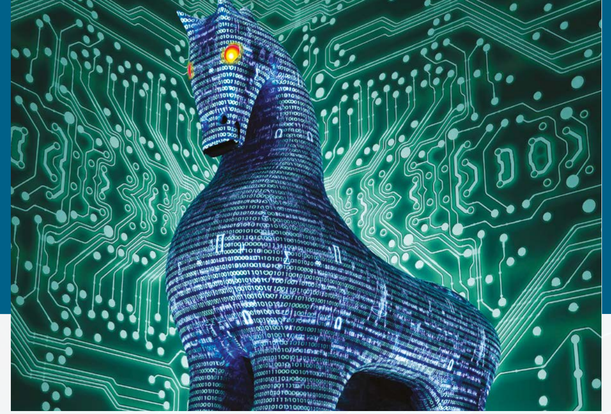
UMFASSENDE ALLGEFAHRENDECKUNG

SCHUTZ DES KONZERNS UND ALLER TOCHTERUNTERNEHMEN

WELTWEITER VERSICHERUNGSSCHUTZ

VOLLER DECKUNGSSCHUTZ IM HOME-OFFICE INKLUSIVE

Deckungsschutz im Home-Office ist bei einigen Anbietern nicht selbstverständlich. Anders ist dies bei der VDMA Cyber-Police. Die Cyber-Versicherung für den Maschinen- und Anlagenbau deckt auch die neue Risikolage im Home-Office ab. Ohne versteckte Ausschlüsse oder zusätzliche Anzeigepflichten. Umfassend, weltweit, zuverlässig.



DECKUNGSUMFANG DER VDMA CYBER-POLICE

VDMA CYBER-POLICE: UMFASSENDER SCHUTZ MIT WELTWEITER GELTUNG

Ganz gleich, wie gut Ihre IT-Sicherheit aufgestellt ist – die Hackercommunity findet neue Einfallstore. Sichern Sie sich ab! Mit einer Cyber-Versicherung, die Ihre Risiken im Zaum hält. Die VDMA Cyber-Police kommt für alle maßgeblichen Dritt- und Eigenschäden auf und deckt auch die Cyber-Risiken im Home-Office ab. Umfassend, weltweit, zuverlässig.

✓

EIGENSCHÄDEN

Abgedeckt sind alle **maßgeblichen Eigenschäden** wie z. B. :

- Betriebsunterbrechungsschäden
- Produktionsausfallschäden
- Rechtsanwaltskosten
- Kosten der Datenwiederherstellung

✓

DRITTSCHÄDEN

Abgedeckt sind alle **maßgeblichen Drittschäden** wie z. B.:

- Ansprüche wegen Nutzungsausfall von gelieferten Maschinen
- Schadenersatzsansprüche wegen Datenmissbrauch

✓

ASSISTANCE-LEISTUNGEN

Umfassende **Unterstützung durch Experten** wie z. B.:

- IT-Forensiker
- Rechtsberatung
- Krisenmanagement
- PR-Beratung

ANGEBOT ANFORDERN

Inhaltsverzeichnis

Einleitung

Cyber-Risiken & IT-Sicherheit

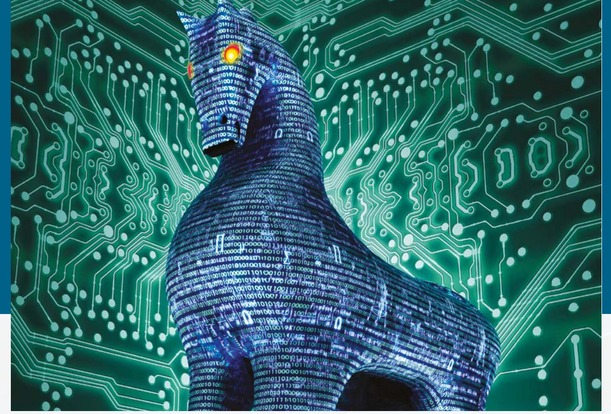
Ransomware & Phishing

IT-Sicherheit im Home-Office

VDMA Cyber-Police (VCP)

VCP-Angebot anfragen

Cyber-Newsletter abonnieren



ASSISTANCE-LEISTUNGEN IM SCHADENFALL

VDMA CYBER-POLICE: NOTFALL-HOTLINE UND EXPERTENTEAM INKLUSIVE

Im Ernstfall kann guter Rat teuer werden. Sorgen Sie vor – mit einer Cyber-Versicherung, die Ihnen im Schadenfall zur Seite steht. Die VDMA Cyber-Police kommt nicht nur für Schäden auf, sie bietet auch wichtige Assistance-Leistungen. Eine Notfall-Hotline unterstützt Sie telefonisch, erfahrene Experten helfen bei der Bewältigung des Vorfalls.

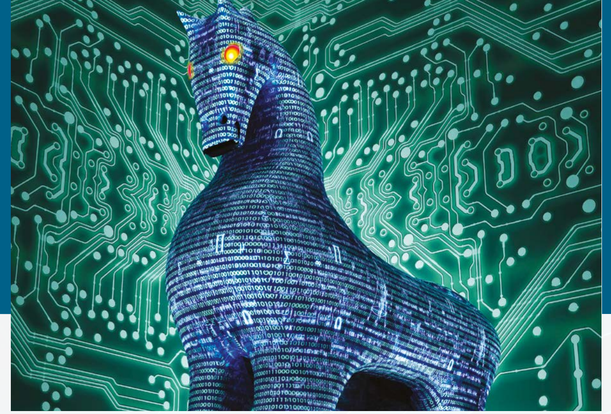
NOTFALL-HOTLINE

Schon beim bloßen Verdacht eines Hackerangriffs sind wir für Sie da. Eine Spezialisten-Hotline unterstützt Sie telefonisch und liefert eine erste Einschätzung.

EXPERTEN-NETZWERK

Im Schadenfall stellen wir Ihnen erfahrene Experten zur Seite, die Ihnen bei der Bewältigung des Vorfalls helfen und Maßnahmen einleiten, um den Schaden möglichst gering zu halten.

ANGEBOT ANFORDERN



VCP-ONLINE-ANGEBOTSTOOL

VDMA CYBER-POLICE: INDIVIDUELLES ANGEBOT EINFACH ONLINE ANFORDERN

Sie haben Interesse an einem Angebot? Gerne! Damit wir Ihr Versicherungsangebot exakt auf die Bedürfnisse Ihres Unternehmens abstimmen können, benötigen wir vorab einige Informationen zur Einschätzung Ihres Cyber-Risikos. Um Ihnen die Übermittlung leicht zu machen, haben wir ein nutzerfreundliches Online-Angebotstool entwickelt. Einfach auf „Angebot anfordern" klicken – Sie werden dann automatisch weitergeleitet.

1

UNTERNEHMENSPROFIL EINMALIG ANLEGEN

2

FRAGEBOGEN VOLLSTÄNDIG AUSFÜLLEN

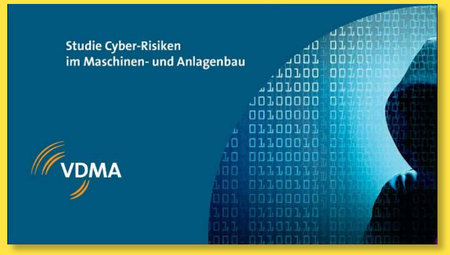
3

„FRAGEBOGEN ABSENDEN" ANKLICKEN

ANGEBOT ANFORDERN

Inhaltsverzeichnis
Einleitung
Cyber-Risiken & IT-Sicherheit
Ransomware & Phishing
IT-Sicherheit im Home-Office
VDMA Cyber-Police (VCP)
VCP-Angebot anfragen
Cyber-Newsletter abonnieren

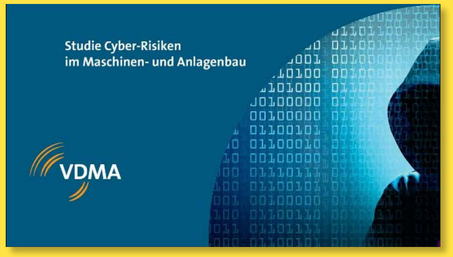
20 ANHANG: STUDIEN + BROSCHÜREN



VDMA STUDIE

CYBER RISIKEN IM MASCHINEN- UND ANLAGENBAU

BESTELLEN



VDMA REPORT

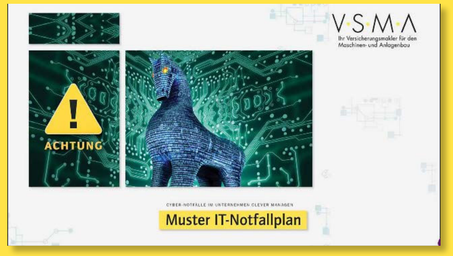
INDUSTRIAL SECURITY REPORT

BESTELLEN

VDMA BROSCHÜRE

NOTFALLHILFE RANSOMWARE

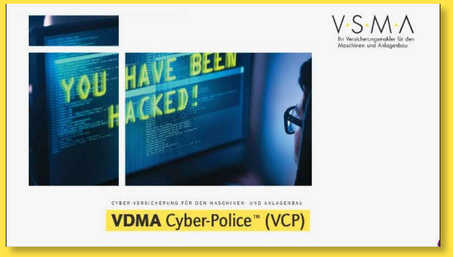
BESTELLEN



VSMA CYBER PLAN

MUSTER IT-NOTFALLPLAN

BESTELLEN



CYBER VERSICHERUNG

VDMA CYBER-POLICE PRODUKTBROSCHÜRE

DOWNLOAD

VSMA CYBER HILFE

MUSTER IT-NOTFALLKARTE

BESTELLEN

Inhaltsverzeichnis

Einleitung

Cyber-Risiken & IT-Sicherheit

Ransomware & Phishing

IT-Sicherheit im Home-Office

VDMA Cyber-Police (VCP)

VCP-Angebot anfragen

Cyber-Newsletter abonnieren

IMPRESSUM | HERAUSGEBER

V·S·M·A
Ihr Versicherungsmakler für den Maschinen- und Anlagenbau

VSMA GmbH
Lyoner Straße 18
60528 Frankfurt a.M.

Telefon: 069 - 6603 •1111
Telefax: 069 - 6603 •1575

E-Mail: service[at]vsma.de
Internet: www.vsma.de

Amtsgericht Frankfurt a. M.
HRB 10572
St.-Nr. 047 247 94805

Vertretungsberechtigte Geschäftsführer:
Jürgen Seiring
Birger Jeurink
Holger Breiderhoff

Rechtlicher Hinweis / Haftungsausschluß:

Bildnachweise:

Fernlernen oder Arbeiten. Videokonferenzkonzept	Stock-Datei-ID:1215748681
Arbeiten während der Isolationsphase	Stock-Datei-ID:1215481936
Konzept der Datensicherheit	Stock-Datei-ID:1214203349
Pirate Schlüssel auf computer-Tastatur	Stock-Datei-ID:460808695
Gefährliche Kapuzen Hacker bricht in Regierung Datenserver....	Stock-Datei-ID:817486228
Malware-Warnhinweise entdeckt	Stock-Datei-ID:1144604134
Kreditkarte phishing	Stock-Datei-ID:533726355
Du warst hacked!	Stock-Datei-ID:502192161
Computer Sicherheit Konzept, Trojaner in elektronischen Umgebung	Stock-Datei-ID:546179030
Technisches Supportkonzept....	Stock-Datei-ID:1199145131

Inhaltsverzeichnis
Einleitung
Cyber-Risiken & IT-Sicherheit
Ransomware & Phishing
IT-Sicherheit im Home-Office
VDMA Cyber-Police (VCP)
VCP-Angebot anfragen
Cyber-Newsletter abonnieren