Stefan Pechardscheck,
Global Head
Technology,
BearingPoint GmbH

Markus Seme,
Geschäftsführer
BearingPoint Österreich,
Director Technology and Services,
BearingPoint GmbH
Österreich

3. **Konfigurations- und Asset-Management** – Ein tragfähiges Konfigurations- und Asset-Management zählt zu den wichtigsten Aspekten, wenn es um Themen wie strukturierte Weiterentwicklung und Absicherung von Leit- und Automatisierungstechnik geht. Gerade bei größeren und komplexeren Umgebungen stößt eine Verwaltung mittels Excel oder eine, die rein auf manueller Erfassung basiert, schnell an ihre Grenzen oder skaliert schlichtweg nicht mehr. Noch dazu sind die Vorteile einer detaillierten und permanent aktuellen System- und Konfigurationsdokumentation nicht nur wichtig bei der Absicherung der Systeme. Auch Regeltätigkeiten wie Systemwartung, notwendige Ausbauten und erste Schritte in Richtung Industrie 4.0 sind ohne diese Daten-Basis nur schwer oder mit großem Risiko zu bewältigen. Wie die eingangs beschriebenen Cyber-Angriffe deutlich machen, bauen komplexere, cyber-physikalische Angriffe immer auf nicht-autorisierte Konfigurationsänderungen auf. Dabei sind oft nicht einmal Sicherheitslücken notwendig, sondern es wird Standardfunktionalität der Automatisierungstechnik quasi für ursprünglich nicht so vorgesehene Anwendungsfälle missbraucht. Wer also solche nicht-autorisierten Konfigurationsänderungen erkennen oder verhindern kann, kann sich auch vor solchen Angriffen wirksam schützen. Moderne, auf Leit- und Automatisierungstechnik spezialisierte Konfigurations- und Asset-Management-Lösungen, bieten neben dem automatisierten Erkennen von unautorisierten Konfigurationsänderungen oder dem Einbringen von nicht autorisierter Hardware in das überwachte Netzwerk, auch noch viele andere Features an. So werden zum Beispiel auch ungewöhnliche Zugriffe oder Datenflüsse auf Komponenten des Steuerungssystems gemeldet oder es können Wartungszugriffe von außerhalb, detailliert überwacht und eingeschränkt werden.
4. **Systematisch pragmatisch** – Da sich Technologien, Infrastrukturen und damit einhergehende Angriffsmöglichkeiten permanent weiterentwickeln, muss ein nachhaltiges Sicherheitskonzept ebenso kontinuierlich verbessert und auf vielen Ebenen angepasst werden. Zahlreiche Normen und Sicherheitssysteme wie die IEC 62443 oder das allgemeinere ISO 27001 adressieren genau diese Herangehensweise, der ganzheitlichen und kontinuierlichen Verbesserungszyklen, sind aber relativ aufwändig in der Umsetzung, wenn man die enthaltenen Empfehlungen und Vorgaben in der vollen Breite mit praktischer und noch dazu betriebswirtschaftlicher Sinnhaftigkeit umsetzen möchte. Wie bei vielen anderen Ansätzen zeigt sich auch hierbei, dass eine Kombination von langfristiger und systematischer Planung, mit pragmatischem, betriebswirtschaftlich sinnvollem Vorgehen am effizientesten ist.

Damit ist gemeint, dass Zeit und Geld primär dort eingesetzt werden sollte, wo gemäß der 80/20 Regel am schnellsten die größtmögliche Verbesserung an Sicherheit geschaffen werden kann. Bestenfalls lässt sich diese Verbesserung dann sogar quantitativ oder qualitativ messen. Gleichzeitig sollen diese Einzelmaßnahmen, sich gegenseitig ergänzend, gut in ein nachhaltiges Gesamtkonzept passen.

5. **Personelle Verantwortung und dediziertes Budget** – Der letzte und vielleicht sogar wichtigste Tipp ist: Richten Sie eine dedizierte personelle Verantwortung für die Cyber-Sicherheit Ihrer Produktionsstätten ein. Wo diese Person oder dieses Team organisatorisch angesiedelt ist, ist dabei nicht so wichtig wie die Anforderung, dass sie unbedingt, zumindest grundlegende Kenntnisse in der Leit- und Automatisierungstechnik mitbringen muss. Darüber hinaus sollte es sich um eine dedizierte Stelle handeln, das heißt um jemanden, der 100 % seiner verfügbaren Zeit dieser Tätigkeit widmen kann.

Eine Implementierung aller oder eines Großteils der beschriebenen Maßnahmen und konkreten Schutzmechanismen verhindert mit hoher Wahrscheinlichkeit die am Anfang des Beitrags beschriebenen Maßnahmen.

Zusammenfassen bleibt daher noch einmal folgendes Fazit festzuhalten:

Die meisten Angriffe, auch auf Industrieanlagen, sind weit weniger komplex als angenommen und mit weit weniger Fachwissen und Ressourcen ausgestattete Attacken. Gegen solche Gefahren ist man auch mit Basismaßnahmen, wie sie etwa die CIS Security Controls empfehlen, schon recht gut abgesichert.

Da sich ein individuelles Security Konzept in jedem Fall immer erst Schritt für Schritt entwickeln und vor allem auch weiterentwickeln muss, ist die Kombination von Basismaßnahmen, auf die dann entsprechend fortgeschrittenere Methoden aufgebaut werden können, ein sinnvoller Ansatz.

Das Wichtigste aber ist: Setzen Sie einen ersten Schritt und bleiben Sie dran!

Stefan Pechardscheck, Markus Seme

Hybrides Arbeiten – welche Maßnahmen jetzt getroffen werden (sollten)

Eine aktuelle Studie zeigt, wie sich Arbeitgeber und -nehmer auf der ganzen Welt auf den digitalen Arbeitsplatz der Zukunft vorbereiten. Was Mitarbeiter zudem wissen müssen, um ihre Arbeitsumgebung im Homeoffice bestmöglich zu schützen.

Mit der Wiedereröffnung der Büros blicken viele auf die pandemiebedingte Fernarbeit als Fallstudie für die Einführung einer flexiblen, hybriden Arbeitsumgebung. Das Aufkommen neuer Varianten führt aber

auch bei Unternehmen zu neuen Unsicherheiten im Zusammenhang mit der COVID-19-Pandemie. Nun geht es darum, einen langfristigen Plan zu entwickeln – ein Arbeitsmodell, das den Bedürfnissen von Mitarbeitern und Geschäftsführung gleichermaßen gerecht wird. Egal, ob es sich dabei um Arbeitsplätze im Büro, im Homeoffice oder um hybride Konzepte handelt. Mit welchen Wünschen, Möglichkeiten und Problemen sich Führungskräfte und Angestellte in dieser Umbruchsphase konfrontiert sehen, hat Entrust in seiner aktuellen Studie „Securing the New Hybrid Workplace“ untersucht.* Ein besonderer Fokus lag dabei auf Fragen zur Absicherung von hybriden Arbeitsplätzen.

Zu den wichtigsten Ergebnissen der Studie gehören:

- Hybride Arbeitsmodelle setzen sich weltweit durch, trotz großer Sicherheitsbedenken: Die überwältigende Mehrheit der Unternehmen geht langfristig zu einem hybriden Arbeitsplatzkonzept über. In Deutschland geben 73 % der Führungskräfte und 85 % der Mitarbeiter an, dass ihr Unternehmen derzeit einen hybriden Ansatz fährt – oder vollständig remote arbeitet und ein hybrides Arbeitsmodell in Betracht zieht. Allerdings berichteten 51 % der Mitarbeiter von teilweise erheblichen Produktivitätseinbußen aufgrund von Problemen beim Netzwerkzugang. Führungskräfte nennen die mangelnde Sicherheit von Heimnetzwerken (21 %) und den Verlust sensibler Unternehmensdaten (16 %) als größte Sorge.
- Besuchermanagement gewinnt auch in Deutschland an Bedeutung: Detaillierte Aufzeichnungen darüber, wer in Büroräumen ein- und ausgegangen ist, haben 2021 eine hohe Priorität: 88 % der Führungskräfte und 87 % der Mitarbeiter halten ein System zur Aufzeichnung und Kontrolle des Besucherverkehrs während der Arbeitszeiten für wichtig.
- Die Datensicherheit im Home Office bringt neue Herausforderungen mit sich: Mitarbeiter arbeiten heute dezentraler als je zuvor, weshalb Unternehmen ihre Datensicherheitskonzepte anpassen müssen. Aber während 84 % der Führungskräfte bestätigen, dass ihr Unternehmen seinen Angestellten Schulungen zum Thema Datensicherheit angeboten hat, nahmen nur 57 % der Mitarbeiter Notiz davon – was auf eine erhebliche Kommunikationslücke hindeutet.

Neue Möglichkeiten des hybriden Arbeitsmodells

Die Studie unterstreicht mit einer überwältigenden Mehrheit von 91 % weltweit den Wunsch von Angestellten nach einem hybriden Arbeitsmodell. Es steht außer Frage, dass Arbeitgeber diesem Bedürfnis nachkommen. 61 % der befragten Führungskräfte in Deutschland gaben zudem an, dass sie bei der Neubesetzung freierwerdender Positionen die Einstellung von neuen Talenten an geografisch unterschiedlichen Standorten in Betracht ziehen. Neue Möglichkeiten

sind gefragt, die Onboarding- und Einarbeitungsprozesse in einem hybriden Arbeitsumfeld abzusichern und zu verbessern.

Was die Absicherung des hybriden Arbeitens angeht, so erklären 84 % der Führungskräfte in Deutschland, dass ihr Unternehmen über eine Richtlinie oder einen formellen Leitfaden verfügt. 93 % geben an, dass in ihren Richtlinien bewährte Verfahren zur Datensicherheit und zum Datenschutz erörtert werden.

Dennoch gibt es viele Sicherheitsbedenken gegenüber hybriden Arbeitsmodellen, die sich zumeist auf das Homeoffice beziehen. So machen sich deutsche Führungskräfte Sorgen um:

- die Sicherheit der Internetverbindung im Zuhause ihrer Mitarbeiter: 21 %
- das Durchsickern sensibler Unternehmensdaten: 16%
- Cyberangriffe durch bösartige Akteure: 24%
- mangelhafte Datenschutzmethoden: 18%
- mangelnde Privatsphäre in der Wohnung: 6%
- Phishing-Angriffe: 6%
- unzureichende Passwortverwaltung: 4%
- Verstöße gegen die Vorschriften: 2%

Die Studie zeigt, dass deutsche Abteilungsleiter als Konsequenz ihre Schulungsmethoden verbessern (57 %), neue Tools für die Zusammenarbeit einführen (39 %) und mobile IDs für Mitarbeiter an entfernten Standorten ausstellen (37 %). Darüber hinaus ergreifen die Führungskräfte im Zusammenhang mit der Einführung hybrider Arbeitsmodelle technologische Maßnahmen zur Kontrolle der firmeneigenen IT-Sicherheit – insbesondere Lösungen für das Identity Access Management (IAM) sind unverzichtbar geworden. Zukunftsfähige IAM-Software muss hybride Umgebungen unterstützen, die sowohl On-Premise-Systeme als auch SaaS-Applikationen nutzen und Unternehmen in die Lage versetzen, nicht nur die Zugriffsrechte ihrer internen Mitarbeiter effektiv zu managen, sondern auch jene von Mitarbeitern in Remote-Arbeit und (bei Bedarf) von externen Partnern aus aller Welt.

36 % der deutschen Unternehmen implementieren Technologien für Einmalpasswörter, 43 % nutzen die biometrische Authentifizierung und 21 % eine mobile Identitätsüberprüfung, um Hackern einen Schritt voraus zu sein und interne Daten zu schützen. Im internationalen Durchschnitt liegen deutsche Unternehmen bei der Einführung zukunftsweisender Authentifizierungstools damit jedoch eher im hinteren Bereich.

Besuchermanagement für mehr Sicherheit in der Büroumgebung

In Zeiten der anhaltenden Pandemie müssen Unternehmen neben der physischen und IT-Sicherheit auch die Gesundheit ihrer Mitarbeiter am Arbeitsplatz in

* Insgesamt wurden 1.500 Führungskräfte und 1.500 Angestellte aus 10 verschiedenen Ländern befragt.

Kieran Hernon,
VP Digital Identity
Sales EMEA & APJ,
Entrust

ihre Vorsichtsmaßnahmen einbeziehen. Die Studie von Entrust belegt eine überwältigende Unterstützung für ein umfassendes Besuchermanagement innerhalb von Organisationen: 89 % der deutschen Führungskräfte und 87 % der Angestellten sprechen sich für ein System aus, das Besucher innerhalb des Bürogebäudes protokolliert und kontrolliert.

Die Gründe für diesen verstärkten Kontrollwunsch von Besuchern sind in erster Linie auf die Vorsicht im Zusammenhang mit COVID-19 zurückzuführen. 80 % der Führungskräfte und 79 % der Mitarbeiter nennen das Risiko der Verbreitung von COVID-19 als wichtigsten Grund für die Einrichtung eines Besuchermanagementsystems. Weitere Gründe sind der Schutz vertraulicher Informationen (43 % der Führungskräfte und 55 % der Mitarbeiter) sowie die Vermeidung von Körperverletzungsdelikten (44 % der Führungskräfte und 28 % der Mitarbeiter).

Steigendes Bewusstsein für Datenschutzbelange

Lange galt es als schwierig, Heimarbeit mit den unternehmensweiten Datenschutzrichtlinien in Einklang zu bringen. Hier scheinen die pandemiebedingten Maßnahmen zu einem Schritt in die richtige Richtung geführt zu haben: 84 % der deutschen Führungskräfte geben an, dass ihr Unternehmen Mitarbeitenden Schulungen zur Datensicherheit angeboten hat – für die überwältigende Mehrheit ist dies als Folge der COVID-19-Pandemie geschehen. Mithilfe von Schulungen können Unternehmen das Risiko von Sicherheitsbedrohungen wie Phishing- und Ransomware-Angriffen drastisch reduzieren, da diese das mangelnde Bewusstsein ihrer Adressaten ausnutzen.

Leider waren sich nur 57 % der Mitarbeiter bewusst, dass ihr Unternehmen Schulungen zum Thema Datensicherheit anbietet – was auf eine mangelnde Kommunikation in diesem Bereich hinweist.

Globale Perspektive

Im internationalen Vergleich sind Studienergebnisse aus einzelnen Ländern besonders interessant. Zu den wichtigsten internationalen Trends und Erkenntnissen gehören:

- Unternehmen in Saudi-Arabien (89 %) und den Vereinigten Arabischen Emiraten (87 %) sind am ehesten bereit, für neu zu besetzende Positionen Talente aus der ganzen Welt zu berücksichtigen. Gefolgt von Unternehmen in den Vereinigten Staaten und Singapur. Hier geben jeweils 73 % der Führungskräfte an, dass sie sich vorstellen könnten, neue Mitarbeiter unabhängig von deren Standort einzustellen.
- Unternehmen in Indonesien integrieren besonders häufig modernste Sicherheitstechnologien in ihre bestehenden Geschäftsabläufe: 75 % der Arbeitgeber geben an, dass sie Einmalpasswörter verwenden, 69 % nutzen biometrische Authentifizierungsmethoden.

- 65 % der Arbeitgeber in Japan waren sich einig, dass sie Datensicherheitsschulungen für das hybride Arbeitsmodell angeboten haben. Aber nur 36 % der Arbeitnehmer stimmen dem zu, was auf mögliche Probleme bei der Durchführung von Schulungen hinweist.

So können Sie Ihre hybride Arbeitsumgebung optimieren:

Unter Berücksichtigung der größten Sorgen vieler Führungskräfte und Mitarbeiter weltweit möchten wir Ihnen folgende, einfach umzusetzende Sicherheitstipps mit auf den Weg geben. So können Sie dazu beitragen, dass IT-Systeme auch im Homeoffice geschützt und Daten sicher bleiben:

- Erstellen Sie eine separate, sichere Internetverbindung für ihre Arbeitsbelange. Die meisten zeitgemäßen Internet-Router für Privatkunden bieten die Möglichkeit, mehr als ein drahtloses Netzwerk einzurichten. Mitarbeiter können so ein separates Netzwerk mit einer höheren Sicherheitsstufe aufsetzen (z. B. unsichtbare SSID, aktiviertes VPN, komplexe Kennwörter usw.).
- Verwenden Sie nur zugelassene Cloud-Dienste. Wenn eine Frist abläuft oder ein Kunde verärgert ist, kann es verlockend sein, unter Zuhilfenahme externer Dienste schnell die notwendige Anfrage zu erledigen. Ob es sich dabei um die Nutzung einer „kostenlosen“ Online-Ressource handelt, um eine Präsentation aufzupeppen, oder um das Hochladen von Inhalten in einen nicht genehmigten Dateifreigabedienst, weil sie zu groß für E-Mails sind – all diese Dienste werden nicht von der Unternehmens-IT geprüft und stellen eine Sicherheitslücke dar.
- Halten Sie Richtlinien für Passwörter ein. IT-Abteilungen können mit Identity- und Access-Management viel dazu beitragen, dass Benutzer und ihre Daten sicher bleiben. Mitarbeiter müssen ihnen aber auf halbem Weg entgegenkommen, indem sie ihre Passwörter sicher verwalten, ihre Geräte regelmäßig updaten und konform mit den Unternehmensrichtlinien halten.
- Trennen Sie berufliche und private Aktivitäten. Einer der Vorteile des Homeoffice ist die Möglichkeit, während der Pausen persönlichen Besorgungen und Erledigungen nachzukommen. Ganz gleich, ob es sich um Online-Shopping, soziale Medien oder persönliche E-Mails handelt: wenn Sie Ihren privaten Laptop, Ihr Tablet oder Ihr Telefon zur Hand haben, ist es besser, alle persönlichen Online-Aktivitäten auf diese Geräte zu beschränken – und damit sicherzustellen, dass die Arbeitsgeräte frei von Cyberangriffen bleiben, die über persönliche Konten erfolgen könnten.

Über die Studie „Securing the New Hybrid Workplace“

„Securing the New Hybrid Workplace“ ist eine Studie des Ponemon Instituts im Auftrag von Entrust mit 1.500 Führungskräften und 1.500 Mitarbeitern aus den Vereinigten Staaten, Kanada, Großbritannien, Australien, Deutschland, Saudi-Arabien, den Vereinigten Arabischen Emiraten, Indonesien, Japan und Singapur. Die Daten wurden im Laufe des Jahres 2021 erhoben. Die Studie untersucht aktuelle Themen wie Best Practices für hybrides Arbeiten, Besuchermanagement in Bürogebäuden und den Einfluss hybrider Arbeitsmodelle auf die Sicherheit am Arbeitsplatz.

Kieran Hernon

1.5 REAKTIONEN

Cybersicherheit braucht Digitalisierung ... oder andersherum?

Eine erfolgreiche Digitalisierungsstrategie von Unternehmen braucht eine angemessene Cybersicherheit. Daraus lässt sich ableiten, dass eine Cybersicherheitsstrategie eine digitale Cybersicherheitsstrategie sein muss, sich am Geschäftsmodell und Digitalisierung ausrichten muss. Und weil die Dynamik der Digitalisierung hoch ist, ist die Verbindung dieser zwei Themenbereiche umso wichtiger.

Das Bundeskriminalamt hat in ihrer Sonderauswertung im Rahmen der Corona-Pandemie die Beschleunigung der Nutzung digitaler Dienste hervorgehoben.

„Die Gesellschaft weicht im Zuge der Corona-Krise vermehrt auf die digitale Welt aus - ein perfekter Nährboden für Cyberkriminelle.“ (BKA, Cybercrime in Zeiten der Corona-Pandemie, 30. September 2020). Die zunehmende Digitalisierung erfordert als logische Konsequenz, kontinuierlich und besser auf Cyberangriffe vorbereitet zu sein.

Diese Entwicklung zeigt, dass der Ansatz, Cybersicherheit und Digitalisierung zu verknüpfen sinnvoll und erfolgversprechend ist. Damit wird Cybersicherheit aus der Expertennische herausgeführt, ganz so, wie immer deutlicher wird, dass Digitalisierung ebenfalls kein reines Expertenthema sein darf. Diesen Gedanken konsequent weitergedacht, bedeutet es vielmehr, dass eine Haltung gegenüber der Cybersicherheit in Unternehmen gebraucht wird, die Cybersicherheit als Teil des Business versteht und nicht als Tradeoff zum Business – Cybersicherheit ermöglicht Digitalisierung.

Denn so, wie Digitalisierung ein kontinuierlicher Prozess ist, ist auch Cybersicherheit ein Aufgabenfeld, welches Unternehmen stetig weiterentwickeln müssen. Ein „Fertig“ wird es weder in der Digitalisierung noch

in der Cybersicherheit geben - es sind Daueraufgaben.

Es lassen sich weitere Verbindungen zwischen den Anforderungen an eine Organisation für erfolgreiche Digitalisierung und für erfolgreiche Cybersicherheit ziehen. So entsteht eine verstärkende Wechselwirkung zwischen Cybersicherheit und Digitalisierung.

Aspekte der Digitalisierung

Beispielhaft soll die Studie des Instituts der deutschen Wirtschaft für Anforderungen der Digitalisierung herangezogen werden. In der Studie (IW, Digitalisierung und mitarbeiterorientierte Führung, 2020) werden drei Megatrends für Digitalisierung aufgezeigt.

1. Zeitliche und räumliche Flexibilität von Beschäftigten
2. Automatisierung, Informatisierung und künstliche Intelligenz
3. Veränderung, Verantwortung, Vertrauen in der Führung

Veränderte mobilere Arbeitsformen sorgen für einen höheren Grad an Handlungsfreiheit und daraus resultierend für mehr Selbstkontrolle und -steuerung, möglicherweise aber auch für eine zunehmende Verunsicherung. Dies zusammen mit der fortschreitenden technologischen Entwicklung sorgt für veränderte Kompetenz- und Aufgabenbereiche. Insbesondere sind Veränderungsbereitschaft und Kreativität erforderlich, um die Innovationskraft von Unternehmen aufrechtzuerhalten und auf sich verändernde Marktentwicklungen schnell und angemessen reagieren zu können. Innovation entsteht durch ausprobieren und Mut, verbunden mit einer konstruktiven Fehlerkultur, in der Fehler frühzeitig erkannt werden und eine korrigierende Reaktion erfolgt.

Überträgt man diese Konsequenzen auf die Anforderungen für Cybersicherheit, so wird deutlich, dass Cybersicherheits-Kompetenz bei jedem einzelnen wichtig ist. Bei der zunehmenden Handlungsfreiheit ist es erforderlich, mögliche Risiken und Grenzen einschätzen zu können, also in der Lage zu sein, Dinge kritisch zu hinterfragen. Digitalisierungskompetenz und Cybersicherheitskompetenz haben also ähnliche Anforderungen, in der eigenverantwortlichen Handeln einen wichtigen Teil ausmacht.

Die veränderte Rolle von Experten

Welch herausragende Rolle Daten in der Digitalisierung und für die Gesellschaft spielen, wird in der Datenstrategie der Bundesregierung deutlich. „Daten bilden die Grundlage der digitalen Gesellschaft. Mehr Daten innovativ, verantwortungsvoll und gemeinwohlorientiert zu nutzen, kann das Zusammenleben in Deutschland, in Europa und in der Welt bedeutsam verbessern und natürliche Ressourcen schützen.“ (Die Bundesregierung, Datenstrategie der Bundesregierung, 27. Januar 2021)

Ralf Kleinfeld,
Information Security
Officer,
Otto (GmbH &
Co KG)