TRANSFORMATION DER ARBEIT ALS CHANCE FÜR WACHSTUM

Wie Unternehmen cybersicheres „New Work“ für ihren Erfolg nutzen können

Die Ereignisse der vergangenen Jahre haben die Art, wie wir arbeiten, grundlegend gewandelt. Heute ist es ein wichtiges Erfolgskriterium für Unternehmen, eine durchdachte Strategie für Telearbeitsplätze zu haben. Nicht nur für mehr Flexibilität, sondern auch im Kampf um wertvolle Fachkräfte ist es für Firmen entscheidend, sich von alten Strukturen zu trennen und die eigene Digitalisierung inklusive der Möglichkeit zum Homeoffice für die Mitarbeitenden voranzutreiben.

Denn mittlerweile ist Remote Work zu einer festen Größe geworden. Es kann praktisch überall dort stattfinden, wo ein Internetanschluss vorhanden ist. Wir haben uns entschlossen, unsere eigenen Erfahrungen mit der Umstellung auf New Work mit Ihnen zu teilen und einen Ausblick zu geben, welche Rolle ortsunabhängiges Arbeiten in Zukunft spielen wird. Zudem erhalten Sie in diesem Ratgeber wertvolle Tipps, wie Sie die Arbeitsplätze so gestalten können, dass sie alle Anforderungen an die Sicherheit erfüllen. Dieses Handbuch hilft Unternehmenslenkern und Administratoren dabei, die wertvollen Firmendaten auch dann zu schützen, wenn die Mitarbeitenden nicht vor Ort, sondern im Homeoffice oder unterwegs tätig sind.

Welche neuen Ansätze und „Lessons learned“ sich aus der Covid-19 Pandemie ziehen lassen

Von heute auf morgen in neue Strukturen

In den Jahren vor der Pandemie haben sich in Deutschland Strukturen hin zu einem mobilen Arbeiten eher gemächlich entwickelt. COVID-19 hat praktisch von heute auf morgen alles geändert. Die Pandemie stellte Unternehmen vor die Herausforderung, Remote Working zu ermöglichen und die dazu erforderlichen Rahmenbedingungen in kürzester Zeit zu schaffen. Diese Ausnahmesituation beeinflusst bis heute die Unternehmen. Nach wie vor arbeiten einige Angestellte mobil von zuhause aus. Gleichzeitig haben wir durch die Erfahrungen der vergangenen Jahre die einmalige Möglichkeit, das so gewonnene Wissen zu nutzen, um uns von starren Arbeitsstrukturen zu verabschieden und den erfolgreichen Einstieg in New Work zu schaffen.

New Work benötigt digitale Geräte – aber wer beschafft sie und wie können sie genutzt werden?

COBO – Corporate Owned, Business Only

Das Unternehmen stellt dem Mitarbeiter digitale Geräte zur Verfügung. Diese dürfen aber ausschließlich beruflich eingesetzt werden, eine private Nutzung ist verboten.

COPE – Corporate Owned, Personally Enabled

Dies ist eine Variante von COBO, erlaubt allerdings die private Nutzung unter bestimmten Bedingungen.

BYOD – Bring Your Own Device

Der Mitarbeiter nutzt sein privates Equipment auch beruflich. Er bezahlt die Anschaffung und erhält in den meisten Fällen vom Arbeitgeber entsprechende Zuschüsse für die Verwendung.

CYOD – Choose Your Own Device

Das Unternehmen bietet dem Mitarbeiter eine Liste von Geräten an, aus der er seine Wunschgeräte auswählen kann. Diese darf er dann sowohl beruflich als auch privat einsetzen. Die Devices bleiben aber im Firmenbesitz.

Die Wichtigkeit von Informationen

Fehlende Informationen verursachen Probleme. Das wissen Unternehmenslenker nicht erst seit der COVID-19-Pandemie, aber dort wurde es besonders deutlich. Mitarbeitende müssen in der Lage sein, auf alle für ihre jeweiligen Tätigkeiten erforderlichen Informationen zuzugreifen und diese auch mit Kolleginnen und Kollegen zu teilen.

Wichtig ist es, dass Angestellten im Homeoffice nach Möglichkeit unternehmenseigene Geräte zur Verfügung gestellt werden. Denn auf den Endgeräten – Laptops, stationäre PCs, Tablets, Smartphones – werden firmenrelevante Informationen geladen, bearbeitet, gespeichert und geteilt. All das erfordert Plattformen, auf denen die Datenintegrität gewahrt wird und gleichzeitig Mitarbeitende, die im korrekten Umgang mit den zum Teil sensiblen Informationen geschult sind. So ist es beispielsweise wichtig, ein Bewusstsein dafür zu schaffen, dass Arbeiten in der privaten Umgebung zuhause keinesfalls bedeutet, dass ein lockerer Umgang mit Unternehmensinformationen angemessen und gestattet ist. Vertrauliche Firmendaten bleiben – unabhängig von dem Ort, an dem sie verarbeitet werden – vertraulich. Diese Erkenntnis muss bei den Angestellten fest verankert sein, damit sie auch außerhalb des Büros verantwortungsvoll mit ihren Aufgaben und den zugehörigen Informationen umgehen.

Planung, Planung und nochmals Planung

Die Situation in der COVID-Pandemie erforderte schnelles Handeln. Aus diesen Rahmenbedingungen und bereits zuvor vorhandenen Krisenplänen schuf ESET ein Aktionsprogramm, das auch heute noch für mobiles Arbeiten Anwendung findet. Denn es erfordert einiges an Organisation, bestehende Abläufe an New Work-Modelle anzupassen und Informationsflüsse so abzubilden, dass sie unabhängig vom Arbeitsort der einzelnen Mitarbeitenden ungebrochen weiter bestehen. Zu Beginn der Krise haben wir daher einen Planungsausschuss eingerichtet, der die Rahmenbedingungen für das Arbeiten außerhalb der eigenen Büroumgebungen geschaffen hat.

Auch über die Pandemie hinaus ist die Zusammensetzung dieses Ausschusses für Unternehmen auf dem Weg zu neuen Arbeitsmodellen eine exzellente Blaupause. Sie zeigt, mit welchen Abteilungen und Kompetenzen eine Abstimmung erfolgen muss, damit alle wesentlichen Rahmenbedingungen für Homeoffice und Mobile Work erfüllt werden können.

Wie sich Strukturen aufbauen lassen, die mobile Arbeitsplätze im eigenen Unternehmen ermöglichen und managen.

Planungsausschuss (bestehend aus Management, Personalabteilung, IT, Verwaltung)

Planung und Realisation von mobilen Arbeitsplätzen, Evaluation, welche Bereiche für mobiles Arbeiten geeignet sind und Schaffung und Bereitstellung der notwendigen Infrastruktur.

Personalabteilung	übernimmt die Kommunikation mit den Mitarbeitenden. Entscheidet bezüglich der Möglichkeiten sowie des Arbeitsumfangs und der Zeiten für mobiles Arbeiten.
Leitung der einzelnen Niederlassungen	Regionaldirektoren und Chief Business Officer / Chief Sales Officer prüfen, welche Bereiche ihrer Niederlassung für mobiles Arbeiten geeignet sind und welche Tätigkeitsfelder mobil angelegt werden können.
Gruppen- und Abteilungsleiter	entscheiden, wer in welchem Umfang im Verantwortungsbereich mobil arbeiten kann. Hier gilt es, die einzelnen Aufgaben genau zu prüfen und anhand der zur Verfügung stehenden mobilen Arbeitsmittel abzuwägen, welche Tätigkeiten ohne Qualitätseinbußen auch remote gestaltet werden können.

Schwierig selbst für Technologieunternehmen

Man könnte meinen, dass Technologieunternehmen bei der Umstellung auf mobiles Arbeiten nicht in Schwierigkeiten geraten können - denn sie sind eigentlich die Experten in Sachen IT. Doch auch in diesem Sektor sollten die organisatorischen Herausforderungen nicht unterschätzt werden.

Wichtig ist, dass für alle Mobile Worker eine geeignete IT zur Verfügung steht. Hier können Unternehmen bereits die Weichen für die Zukunft stellen. Wer beispielsweise Desktops mit nach Hause nehmen muss, verlagert die Arbeit einfach von einem zu einem anderen Ort. Hier trifft der Begriff des mobilen Arbeitens nur bedingt zu. Für diese Aufgabe passender sind Notebooks, denn damit lassen sich Aufgaben tatsächlich ortunabhängig erledigen. Hier ist es entscheidend, auf die Leistungsdaten der Systeme zu achten, damit das mobile Gerät zu den jeweiligen Aufgaben passt. Wer zum Beispiel vorwiegend Texte erstellt, benötigt weniger Performance als derjenige, der mit leistungshungrigen Anwendungen arbeiten muss. Zudem gilt es abzuwägen, ob nicht zum Beispiel ein weiterer Monitor angeschafft werden sollte. Das ermöglicht das produktive Arbeiten im Büro sowie auch in den eigenen vier Wänden an einem großen und übersichtlichen Bildschirm.

Zu prüfen ist außerdem, ob weitere Geräte für die Arbeit im Homeoffice zur Verfügung gestellt werden müssen. Sind eventuell einige Mitarbeitende darauf angewiesen, auch beim Remote Working drucken zu können? Wenn ja, muss evaluiert werden, ob es genügt, dass die Angestellten das zentral über Abteilungsdrucker im Büro erledigen können, oder eventuell eigene Drucker zu Hause benötigen. Eine genaue Prüfung der IT-Infrastruktur bringt die notwendige Sicherheit, dass auch mobil arbeitende Kollegen über die Ausstattung verfügen, um ihre Aufgaben gut erfüllen zu können.

Ein solcher Check sollte sich nicht ausschließlich auf die Hardware erstrecken. Denn in sehr vielen Fällen müssen Beschäftigte im Homeoffice auf unternehmensinterne Ressourcen zugreifen. Im ERP, im CRM und auf Netzlaufwerken liegen üblicherweise geschäftskritische Daten, die nicht einfach für externe Zugriffe freigegeben werden dürfen. Dazu müssen VPN-Lizenzen angeschafft und verwaltet werden. Zusätzlich ist eine Zwei-Faktor-Authentifizierung erforderlich, damit etwa bei einem Passwortdiebstahl kein unberechtigtes Einloggen durch Dritte erfolgen kann. Daten, die lokal auf mobil genutzten Computern gespeichert werden, müssen zusätzlich verschlüsselt werden. Beides ist auch deshalb essenziell, damit Unternehmen sensible Daten auch außerhalb der eigenen Büroräume gemäß den Vorgaben der EU-Datenschutz-Grundverordnung (DSGVO) schützen.

Daniel Chromek, ESET CISO

> *„Durch COVID-19 haben wir auf dem harten Weg lernen müssen, wie mobiles Arbeiten für einen hohen Anteil der Belegschaft schnell und sicher ausgerollt werden kann. Von dieser Erfahrung profitieren wir noch immer – nehmen Sie doch ebenfalls etwas davon mit auf den Weg zu Ihrer Transformation in Richtung New Work!“*

Sicherheit an erster Stelle

ESET setzt seit Jahren – also schon lange vor der Pandemie – auf erhöhte Sicherheit bei mobilen Geräten und deren Daten. Der Schutz des Endpoints und der E-Mail-Postfächer reichte schon lange nicht mehr aus. Deswegen setzte ESET auf das Prinzip des Multi Secured Endpoints.

Der Multi Secured Endpoint sichert mobile Geräte - überall

Mit dem sogenannten Multi Secured Endpoint legen IT-Verantwortliche einen wichtigen ersten Grundstein ihrer IT-Security im Sinne von ▶ Zero Trust. Dieser sichert so Endpoints weit besser ab als andere Systematiken zuvor. Und: Es spielt nun keine Rolle mehr, ob sich das Gerät oder der Anwender im IT-sicheren Bürogebäude befindet. Im Zusammenspiel vom vorhandenen Malware-Schutz mit einer Festplattenverschlüsselungs- und Multi-Faktor-Authentifizierungslösung sowie Cloud Sandboxing verwandeln Administratoren PCs und Laptops in sogenannte „gehärtete Endpoints". Diese benötigen keine Serverstrukturen oder Verbindungen zum Netzwerk, um optimal gesichert zu sein.

Verschlüsselung stoppt Datenschnüffler

Alle auf dem Endpoint gespeicherten Informationen sollten vor neugierigen Blicken oder im Verlustfall geschützt sein. Mit dem Einsatz einer Verschlüsselung schlagen Verantwortliche zwei Fliegen mit einer Klappe. Cyberkriminelle können mit den codierten Daten nichts anfangen und gleichzeitig kommt das Unternehmen Anforderungen aus der Datenschutzgrundverordnung nach. Voraussetzung für den Erfolg der Verschlüsselung ist die Akzeptanz des Anwenders. Deswegen sollte die Lösung bei ihrer täglichen Arbeit kaum „spürbar" und zuverlässig arbeiten.

Cloud Sandboxing hält das Postfach sauber

Das Entdecken schädlicher E-Mails und deren Anhänge oder Downloads ist ein wichtiger Eckpfeiler für optimale Sicherheit. Gerade der Empfang von Office-Dokumenten, PDFs und zuweilen auch ausführbaren Dateien gehören zum Alltag in Büros. Nichts wäre schlimmer, als wenn durch dieses Schlupfloch beispielsweise Ransomware eindringt, alle Daten ungewollt verschlüsselt und unzugänglich macht. Abhilfe schaffen in diesem Punkt Lösungen mit einer cloudbasierten Sandbox. Suspekter und potenziell gefährlicher Binärcode wie Ransomware, Advanced Persistent Threats und Exploits wird in einer gesicherten Umgebung ausgeführt und erst bei negativem Befund in das Postfach übermittelt.

Daten- und Netzwerkzugriff nur mit Multi-Faktor-Authentifizierung

Für jeden Administrator ist es ein Albtraum, wenn sich jemand ins Netzwerk einloggt oder Daten aufruft, dessen Identität nicht eindeutig geklärt ist. Deshalb sollte eine Multi-Faktor-Authentifizierung grundsätzlich implementiert werden. Es befinden sich eine Reihe von Lösungen auf dem Markt, die einfach zu handhaben und kostengünstig in der Anschaffung sind. Beispielsweise ebnen professionelle Softwareprodukte den sicheren Zugang zu sensiblen Informationen und Netzwerkumgebungen. So lassen sich in weniger als einer Viertelstunde komplette Netzwerke mit tausenden von Rechnern ausstatten. Zusätzliche Hardware-Anschaffungen sind unnötig, bestehende Smartphones lassen sich per App, FIDO-Sticks oder andere Token problemlos integrieren.

▶ Lesen Sie mehr darüber, wie Sie Ihre Remote-Mitarbeitenden schützen können (in englischer Sprache).

Die Krise als Wegbereiter

Sicherlich hat die Krise auch uns eine Menge Ärger bereitet. Wir mussten neue Prozesse und Lösungen implemetieren, von denen wir überzeugt sind, dass sie uns in Zukunft helfen werden. So starteten wir zum Beispiel mit der Verwendung elektronischer Unterschriften, hoben unser Online-Recruiting-Verfahren auf ein neues Niveau und verbesserten unsere Fernverwaltungsfunktionen. Wir haben nicht nur gelernt, wie wir aus der Ferne arbeiten können, ohne ein einziges wichtiges Projekt absagen zu müssen, sondern auch, wie wir damit noch produktiver sein können. Das ist etwas, das uns auch auf lange Sicht helfen und voranbringen wird.

Wir wussten bereits vor der Pandemie, dass sich viele unserer Mitarbeitenden mehr Flexibilität wünschen. Jetzt sind wir in der Lage, diese Bedürfnisse auch zu erfüllen. Damit können unsere Angestellten ihr Privat- und Berufsleben besser miteinander in Einklang bringen und sind zufriedener. Wir profitieren von höherer Produktivität und werden noch stärker als attraktiver Arbeitgeber wahrgenommen – im Kampf um wertvolle Fachkräfte ein wichtiger Pluspunkt für unser Unternehmen. Wir bei ESET sind davon überzeugt, dass ein vollständig digitalisierter Arbeitsplatz die Zukunft ist. Und sind bereits auf dem Weg dorthin.

Neue Bedrohungen im Spiel

Ethik und Moral sind nichts für Cyberkriminelle. Krisen und Umbrüche sind für sie ideale Gelegenheiten, um ihre Angriffe zu starten. Sie machen es sich zunutze, dass die Mitarbeitenden in solchen Fällen besonders gestresst oder sorglos sind. Auch der Umgang von Angestellten mit neuen, und für sie oft ungewohnten Tools im Homeoffice oder beim mobilen Arbeiten ist ein idealer Nährboden für das Treiben der Hacker. Das hat sich bereits während der Pandemie deutlich gezeigt. „Kriminelle haben schnell die Gelegenheit ergriffen, die Corona-Krise auszunutzen, indem sie ihre Arbeitsweise angepasst oder neue kriminelle Aktivitäten entwickelt haben", sagt Catherine de Bolle, Executive Director bei Europol, ▶ in einem Whitepaper. Auch zahlreiche Studien belegen die Gefahr: „Die Pandemie hat nochmals deutlich vor Augen geführt, welche Bedeutung funktionierende und sichere IT-Infrastrukturen haben", so etwa ▶ das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Unsere Erfahrungen bestätigen das auch heute noch. Beispielsweise entdeckt die ▶ ESET Telemetrie seit der Pandemie weit mehr Phishing-E-Mails als jemals zuvor. Einige der Absender verwenden sogar Namen und Kontakte von echten Mitarbeitenden und fordern die Empfänger auf, betrügerische Rechnungen zu bezahlen, bestimmte Aufgaben auszuführen oder ihre Kontodaten mitzuteilen.

Homeoffice bleibt wichtig

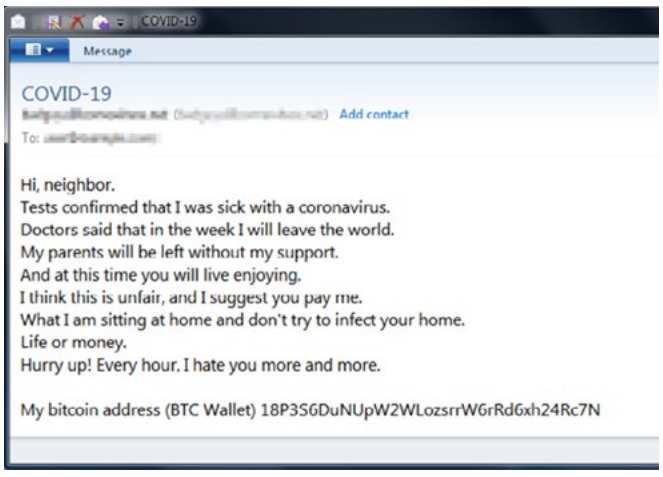
Eine Studie des ▶ Ifo-Instituts von Anfang September 2022 zeigt, dass derzeit fast 25 Prozent aller Beschäftigten in Deutschland die Möglichkeit des mobilen Arbeitens haben. Wenn man die einzelnen Branchen betrachtet, ergibt sich teilweise ein noch deutlich höherer Prozentsatz: So arbeiten Beschäftigte in den Bereichen IT- und Informationsdienstleistung sowie Unternehmensberatungen zu rund 70 Prozent im Homeoffice, während das produzierende und das Gast-Gewerbe mit Anteilen bis hinunter zu einem Prozent das Schlusslicht bilden.

Insgesamt beobachten die Marktforscher des Ifo-Instituts einen anhaltend stabilen Trend zur mobilen Arbeit, obwohl im Frühjahr 2022 die gesetzlichen Vorgaben im Rahmen der Covid-19-Pandemie entfallen sind. „Offenbar setzen Unternehmen und Beschäftigte dauerhaft auf Homeoffice", sagt Jean-Victor-Alipour vom ifo Institut.

Gefahren aus dem Web nehmen nicht ab

Auch in der Phase der abklingenden Pandemie ist das Thema Coronavirus noch immer ein probater Köder in Phishing-Mails. Vermeintlich seriöse Online-Shops setzen beispielsweise auf medizinischen Bedarf für Privatanwender. Sie lassen die Nutzenden bezahlen, ohne ihnen danach die bestellte Ware zu schicken. Dieses „Geschäftsmodell" wird jetzt auf andere Bereiche ausgedehnt, da die Kriminellen ihre für die finsteren Machenschaften geschaffene Struktur weiter nutzen und ihre Betrugsmaschen nun in neuen Varianten durchführen.

Das Problem erstreckt sich nicht nur auf das private Umfeld, sondern auch auf geschäftliche E-Mail-Adressen. Die sogenannten BEC-Angriffe (Business Email Compromise) haben deutlich zugelegt. Unternehmen werden vermehrt zu Opfern von Ransomware- und Malware-Angriffen. Immer häufiger nutzen Kriminelle die Arglosigkeit von Mitarbeitenden im Homeoffice aus, um sich über diese menschliche Schwachstelle Zugang zu Firmennetzen zu verschaffen. Auch hier ist es deshalb äußerst wichtig, die Belegschaft für die Möglichkeit solcher Angriffe zu sensibilisieren. Denn selbst vermeintlich harmlos aussehende E-Mails können zu enormen Schäden führen.



▶ Erfahren Sie mehr darüber, wie gefälschte E-Mails zunehmend zum Problem werden.

Wenn vermeintliche Banken oder Behörden mailen

Gerne werden Fake-Mails von Kriminellen auch mit dem Absender von Banken oder Behörden versehen. Aus dem einfachen Grund: Die meisten Menschen bewerten diese Organisationen als vertrauenswürdig, weshalb entsprechende Mails von vielen Anwendern schneller geöffnet oder Links darin angeklickt werden. Das Fatale daran ist, dass viele der gefälschten Nachrichten nicht nur auf den ersten Blick echt aussehen, sondern vielfach auch Elemente (Logos, Schriftzug, Geschäftsangaben, etc.) der echten Institution verwenden. Wer hier im Homeoffice nicht aufmerksam bleibt, öffnet schnell Malware das Tor zum mobilen Arbeitsplatz und damit letztlich zum Firmennetzwerk.

> *„Die Angreifer machen sich die Situation zunutze, dass zuhause arbeitende Menschen sorgloser agieren.*
> Daniel Chromek, ESET CISO

Gefährliche Apps

Neben Computern sind Smartphones und Tablets einer besonderen Gefährdung ausgesetzt. Denn zusätzlich zu E-Mails mit manipulierten Links sind Apps an sich ein nicht zu unterschätzender Risikofaktor. Gerade für Android werden die kleinen Anwendungen auch aus wenig zuverlässigen Quellen angeboten. Manche Apps täuschen eine Funktionalität vor, die sie im Grunde nicht erfüllen oder diese Funktion nicht ihre primäre Aufgabe ist. Unter dem Deckmantel einer Navigation beispielsweise kann ein Banking Trojaner eingeschleust werden, der das Smartphone oder Tablet ausspioniert und bei Banking-Aktivitäten zuschlägt.

Warum Phishing so effektiv ist

▶ Der Digitalverband Bitkom schätzt den jährlichen Schaden durch Diebstahl, Spionage und Sabotage für die deutsche Wirtschaft auf 223 Milliarden Euro. Ein Großteil der Attacken beginnt mit Social Engineering, wozu auch das Phishing zählt. Ein falscher Klick des Mitarbeitenden kann bereits genügen, damit ein Angriff Erfolg hat. Im Vergleich zu anderen Cyber-Attacken ist der Aufwand der Kriminellen für Phishing oft sehr gering. Ausgefeilte Programmierkenntnisse sind kaum notwendig. Daher ist es wenig überraschend, dass laut ESET Threat Report T1 2022 die Zahlen an betrügerischen E-Mails um 37 Prozent von Januar bis April nahezu explodiert sind (im Vergleich zu September bis Dezember in 2021). Die Zahl der blockierten Phishing-URLs stieg den Malware-Forschern zufolge fast genauso stark an. Dass die Betrugsmasche so effektiv funktioniert, liegt in seiner Ausgestaltung: Cyberkriminelle nutzen zum einen Spoofing-Taktiken, um sich als rechtmäßige Absender einer Mail auszugeben. Zum anderen setzen sie auf Social-Engineering-Techniken, die Empfänger zum spontanen Handeln bewegen sollen, ohne vorher die Folgen zu bedenken.

Mobiles Arbeiten – aber sicher!

Trotz aller beschriebenen Gefährdungen lässt sich Remote Working sicher gestalten. Zumal die Vorteile für Unternehmen und Mitarbeitende deutlich überwiegen. Die flexible Ausrichtung der Arbeit ermöglicht es den Firmen, anfallende Aufgabenspitzen dann abzufangen, wenn sie anfallen. Angestellte sind in der Regel motivierter, wenn sie sich ihre Arbeit freier einrichten können, und liefern bessere Ergebnisse. Die Belegschaft profitiert ebenfalls deutlich, da sie auf diese Weise eine bessere Work-/Life-Balance erzielen können. Wie aber sollten Unternehmen vorgehen, um sichere und flexible Arbeitsumgebungen zu schaffen?

Bewerten Sie, wie sich mobiles Arbeiten auf Ihren Betrieb auswirkt

Modern Work hat sich – wie die Analyse des ifo-Instituts gezeigt hat – zu einem festen Bestandteil in unserem Arbeitsleben entwickelt. Doch die Umsetzung im Unternehmen birgt einige Klippen, die umschifft werden wollen. Falls Sie noch keine Homeoffice-Option anbieten oder aber die Ausweitung von Mobile Work planen, gibt es einige Fragen, die Ihnen helfen, die erforderlichen Rahmenbedingungen zu erkennen.

Diese Fragen helfen bei der Umsetzung von Homeoffice und Co.

- Welche Prozesse müssen angepasst werden oder können nicht mehr so umgesetzt werden, wie sie gerade ablaufen? Warum ist das so?
- Ist Ihre IT-Architektur in der Lage, die Geschäftsabläufe des Unternehmens auch auf mobile Arbeitsplätze zu transferieren?
- Fördert die Homeoffice-Option für ihre Mitarbeitenden die Digitalisierung Ihres Unternehmens und optimiert sie dabei auch weitere Prozesse?
- Warum wäre es für Ihre Firma vorteilhaft/nachteilig, wenn es mobile Arbeitsplätze beziehungsweise Homeoffice gäbe (alternativ: oder mehr mobiles Arbeiten angeboten würde)?
- Wäre es sinnvoll, die neuen Strategien und Prozesse, die Ihr Unternehmen bereits in Bezug auf mobiles Arbeiten eingeführt hat, weiter zu verbessern?
- Wenn ja, welche Instrumente und Maßnahmen unterstützen diese Arbeitsweise und wären auch für die Zukunft eine gute Investition?
- Wie nimmt die Unternehmensleitung die Erfahrungen mit der Digitalisierung wahr?
- Wie nehmen Ihre Mitarbeitenden diese Arbeitsweise wahr?

Prüfung des Business-Plans und der New Work-Strategie

Mobiles Arbeiten und Digitalisierung gehen Hand in Hand. Daher ist es für ein Unternehmen wichtig zu schauen, wie sich die Prozesse mit der bestehenden Ausrichtung der Geschäftstätigkeit in Einklang bringen lassen. Ob eine weitere Digitalisierung zusätzliche Chancen offeriert oder nur Selbstzweck ist, muss sorgsam geprüft werden. Meist geht eine solche Entwicklung mit einer geringeren Abhängigkeit von der Arbeitsstätte einher.

Das klassische Beispiel dafür ist das Archiv: In Form von papiernen Unterlagen, die in einem oder mehreren Räumen im Unternehmen aufbewahrt werden, schränkt es verschiedene Freiheitsgrade ein. Mitarbeitende müssen vor Ort sein, um auf die Informationen zugreifen zu können und oftmals ist die Suche nach bestimmten Unterlagen schwierig und langwierig. Digitale Archive hingegen bieten Zugriff von nahezu überall und erleichtern die Suche und die Zuordnung von Dokumenten durch intelligente Funktionen wie das Tagging. So ermöglicht die Digitalisierung nicht nur hybrides Arbeiten der Beschäftigten, sondern beschleunigt gleichzeitig Prozesse durch schnelleres Auffinden relevanter Dokumente.

Sie sollten sich jetzt auf Prozesse konzentrieren, die bereits in sich durch die Digitalisierung profitieren. Gibt es Projekte, die für das Unternehmen von entscheidender Bedeutung sind und die bisher nicht in die digitale Umgebung umgewandelt oder übertragen werden konnten? Bieten diese Prozesse oder entsprechend abgewandelte Workflows gar neue Chancen für die Geschäftstätigkeit des Unternehmens? Wie verschafft New Work Ihnen und Ihren Mitarbeitenden gleichzeitig Vorteile? Es ist wichtig zu erkennen, dass neue Strukturen nicht mehr Arbeit oder die Abkehr von profitablen Pfaden bedeutet, sondern Chancen in sich tragen, mit einer Anpassung der Geschäftstätigkeit und höherer Produktivität durch motivierte Angestellte die Resultate am Ende des Geschäftsjahres signifikant zu verbessern. Dieses Potenzial will genutzt werden.

Wie Sie mit Ihrem Vorstand über Cybersicherheit und Budgets sprechen können

Cybersicherheit ist der Schlüssel zur Digitalisierung

Digitale Lösungen können sicherlich neue Businessfelder eröffnen und die bestehenden Geschäftstätigkeiten stabilisieren. Zudem ermöglicht die Digitalisierung eine bessere Positionierung im Wettbewerbsumfeld. Ein unzureichender Datenschutz hingegen kann hierbei zu enormen Daten- und Umsatzverlusten führen und das Vertrauen in das Unternehmen sowie seinen Ruf insgesamt schädigen. Nicht zuletzt sieht die DSGVO empfindliche Strafen vor, wenn Sie fahrlässig personenbezogene Daten leaken. Daher ist eine umfassende Absicherung die Basis für eine erfolgreiche Digitalisierung.

Die Praxis überzeugt

Legen Sie konkrete Statistiken vor, wie die Internetkriminalität zunimmt und wie bereits ein falscher Klick dem Unternehmen schaden kann. Um zu beweisen, wie gefährlich beispielsweise Phishing sein kann, führen Sie interne Tests durch und senden Sie E-Mails (natürlich ohne schädlichen Inhalt) zu Testzwecken an ihre Mitarbeiter und werten dann aus, wie viele von ihnen auf einen Link klicken und so dem von Ihnen ausgeworfenen Köder folgen. Versuchen Sie auch, einen White Hat Hacker zu beauftragen, in das Netzwerk Ihres Unternehmens einzudringen. So lässt sich eindrucksvoll in der Praxis zeigen, welche Sicherheitslücken geschlossen werden müssen.

Holen Sie die Belegschaft mit ins Boot

Erstellen Sie interaktives Schulungsmaterial, um das Bewusstsein für Cybersicherheit in Ihrem Unternehmen zu schärfen. Gestalten Sie dieses praxisnah und leicht verständlich, damit die zu vermittelnden Botschaften auch bei den Angestellten verankert werden.

In kleinen Schritten zur Digitalisierung

Wenn Ihr Unternehmen noch nicht oder kaum digitalisiert ist, sollten Sie diesen Prozess in kleinen Schritten planen. Der Wunsch nach einer schnellen und umfassenden Umsetzung, die möglichst viele Prozesse und Workflows optimiert, ist meist vorhanden. Genau das führt jedoch oft dazu, dass am Ende nichts von Alledem umgesetzt wird. Starten Sie daher behutsam.

Bedenken Sie, dass jede kleine Veränderung wichtig ist und dabei hilft, das große Ganze zu optimieren. Entwickeln Sie eine Strategie für den digitalen Arbeitsplatz und behalten Sie dabei auch immer die Optionen für Homeoffice mit im Auge. New Work bedeutet hybrides Arbeiten, die Möglichkeit, im Büro und zuhause gleichermaßen gut die anfallenden Aufgaben erledigen zu können. Ein guter Einstieg ist die Buchhaltung. Digitale Prozesse sparen Papier, erleichtern die Zuordnung von Abläufen und bieten sich für Working 4.0 geradezu an. Auf diese Weise können Sie Ihre Finanzen jederzeit und von überall aus verwalten - und wenn das gesamte Unternehmen im Worst Case plötzlich an einem anderen Ort arbeiten muss, ist die digitalisierte Buchhaltung mit allen Informationen immer und überall vorhanden.

Generell ist es für eine erfolgreiche Digitalisierung wichtig, Lösungen zu finden, die Prozesse ortsunabhängig gestalten. So gewinnt das Unternehmen an Flexibilität und auch Mobile Work ist problemlos möglich.

Stellen Sie Ihre Lieferanten und Geschäftspartner auf den Prüfstand

Kein Unternehmen arbeitet heute komplett allein und unabhängig. Es ist vielmehr in eine Kette von Lieferanten, Geschäftspartnern, Kunden und vielleicht auch Subunternehmern eingebunden. Das bedeutet, dass viele zu digitalisierende Prozesse auch über Schnittstellen zu den externen Partnern verfügen müssen. Digitalisierung als Insellösung schafft selten den gewünschten Effekt. Wer Prozesse optimieren möchte, sollte auch über den Tellerrand des eigenen Unternehmens hinausblicken und evaluieren, was getan werden muss, um den Workflow im Verbund mit Lieferanten und Kunden zu optimieren. In welcher Form kommen Aufträge in das Unternehmen? Bereits digital oder auf Papier? Ist es erforderlich, Dokumente in Papierform zuerst zu digitalisieren und einem Dokumenten-Management zuzuführen, bevor sie verarbeitet werden können? Das sind Fragen, die geklärt werden müssen, um den eigenen Grad der digitalen Möglichkeiten auszuloten und geeignete Maßnahmen ergreifen zu können.

Fragen an Ihre Lieferanten und Geschäftspartner

- Nutzen Sie bereits digitale Workflows und wenn ja, wie sind die externen Schnittstellen gestaltet?
- Wie können wir unser System / geplantes System an Ihre Prozesse anbinden, sodass eine Zusammenarbeit ohne Medienbrüche möglich wird?
- Ist der Prozess, den Sie für unser Unternehmen durchführen, ausreichend gegen Cyberkriminalität abgesichert?
- Besteht die Möglichkeit, externe und interne Prozesse zu synchronisieren, um Workflows zu optimieren?
- Verfügen Sie über eine Liste von Lieferanten für kritische Prozesse?
- Ist der Prozess, den Sie für unser Unternehmen erbringen, durch das Risiko von Ausfällen bei anderen Zulieferern beeinträchtigt?
- Wenn ja, haben Sie Maßnahmen ergriffen, um das Risiko von Ausfällen bei anderen Lieferanten, die an den Lieferungen an unser Unternehmen beteiligt sind, zu minimieren?
- Ist Ihr Personal in Sicherheitsfragen / rund um den Datenschutz ausreichend geschult?

Sicherheitslösungen an die Digitalisierung von Prozessen anpassen

Die Verlagerung von Geschäftsprozessen auf die digitale Ebene kann zwar Abläufe signifikant optimieren und New Work effizient unterstützen, birgt aber gleichzeitig zusätzliche Risiken für die Cybersicherheit. Daher sollte Ihre Aufgabe nicht nur darin bestehen, einen hohen Digitalisierungsgrad mit damit verbundener hoher Effizienz zu installieren, sondern auch die Unternehmens- und persönlichen Daten entsprechend zu schützen. Auch eine angemessene Konnektivität ist ein Muss - ein virtuelles privates Netzwerk (VPN) ist daher unerlässlich, um den erhöhten Sicherheitsrisiken zu begegnen. Alle remote Arbeitenden sollten über eine VPN-Lizenz verfügen, um eine sichere Verbindung zum Unternehmensnetz herstellen zu können. Nur so lässt sich gewährleisten, dass unternehmenskritische Daten dort bleiben, wo sie hingehören: in die befugten Hände der jeweiligen Mitarbeitenden!

Eine weitere Voraussetzung für einen effektiven, dezentralen und digitalisierten Arbeitsplatz ist, dass die Beschäftigten über geeignete Gerate verfügen, die sie auch von zu Hause aus nutzen können. Was aber, wenn Ihr Unternehmen im Moment keine neuen Laptops oder Tablets anschaffen kann?

▶ Überlegen Sie in diesem Fall, unter welchen Bedingungen die Mitarbeiter ihre persönlichen Gerate wie Laptops, Smartphones, Desktops und Tablets verwenden dürfen.

Entscheidend ist, dass jedes dieser Devices dann mindestens mit einem aktuellen Malware-Schutz abgesichert wird. Sicherheitsexperten empfehlen sogar eine vollwertige, mehrschichtige Endpoint-Sicherheitslösung eines renommierten Anbieters – der Einsatz kostenloser Antivirusprogramm reicht heutzutage nicht mehr aus und ist selten zentral administrierbar.

Gerade diese nicht vom Unternehmen gemanagten Geräte stellen die IT-Abteilung in puncto Sicherheit vor besondere Herausforderungen. Nicht zuletzt bedeutet dies manuelle Mehrarbeit verbunden mit erheblichen Folgekosten. Wenn betrieblich genutzte Privatgeräte von Cyberkriminellen für Angriffe auf Ihr Firmennetz genutzt werden, kann der durch die Attacke angerichtete Schaden immens sein und im schlimmsten Fall Ihr Unternehmen ruinieren. Deshalb gilt auch in Zeiten knappen Budgets: nicht an der falschen Stelle – nämlich der IT-Sicherheit – sparen.

Cybersecurity-Grundlagen für einen effektiven digitalisierten Arbeitsplatz

- Automatisierte und standardisierte Umgebung für einfache Fernverwaltung. Nach Möglichkeit sollten alle eingesetzten IT-Geräte durch die IT-Abteilung von der Ferne aus zentral verwaltet werden. Nur so lässt sich gewährleisten, dass immer alle erforderlichen Patches und Sicherheitsanwendungen installiert sind.
- Einsatz einer zuverlässigen Endpoint-Sicherheitslösung, die für Unternehmens- und ggf. auch für Privatgeräte verwendet werden kann.
- Eine zuverlässige lokale Festplattenverschlüsselung bei Mobilgeräten, damit sensible Daten bei Verlust oder Diebstahl nicht ausspioniert werden können.
- Eine detaillierte Überwachung jeder App und Anwendung von einer zentralen Management-Konsole aus.
- Einsatz ausschließlich starker Passwörter, unterstützt durch Multi-Faktor-Authentifizierung und durch effektive Gruppenrichtlinien, die Zugriffe regeln.
- Schaffung hybrider Umgebungen durch die Kombination von On-Premesis- und Cloud-Services, um den besten Effekt zu erzielen.

Anpassungen der Sicherheitslösungen an New Work

Wie Sie mobiles Arbeiten und Videokonferenzen schützen

- Achten Sie darauf, dass nur autorisierte Personen an Meetings teilnehmen. Richten Sie Benutzergruppen ein oder beschränken Sie den Zugang nach Internetdomains.
- Setzen Sie sichere Passwörter für Meetings und betten Sie das Passwort nicht in den Link zur Besprechung ein. Denn das birgt die Gefahr, dass das Passwort leicht abgefangen werden kann.
- Lassen Sie die Teilnehmer vor dem Zugang zum digitalen Besprechungsraum warten und genehmigen Sie die Verbindung für jeden Einzelnen. Denn je größer eine Besprechung ist, desto höher die Wahrscheinlichkeit, dass ein ungebetener Gast auftaucht, der versucht, sich in der Masse zu tarnen.
- Verschlüsseln Sie auch das Video mit der Sprachübertragung selbst, denn einige Dienste verschlüsseln nur den Chat!
- Begrenzen Sie den Dateiaustausch und erlauben Sie keinesfalls den Versand ausführbarer Dateien. Das gilt besonders für Konferenzen mit Externen. Denn falls deren Systeme von Maleware befallen ist, könnten diese sonst nur allzu leicht übertragen werden.
- Wählen Sie aus, was Sie auf Ihrem Bildschirm mit anderen teilen möchten. Beschränken Sie sich auf die notwendige Anwendung oder das notwendige Fenster und geben Sie keinen Einblick auf Ihren gesamten Desktop. So verhindern Sie, dass versehentlich allen Teilnehmern vertrauliche Informationen offenbart werden.
- Überprüfen Sie die Datenschutzrichtlinien des von Ihnen genutzten Dienstes. Es ist möglich, dass kostenlose Apps Ihre Daten sammeln und verkaufen, um die Bereitstellung des Dienstes zu finanzieren - Sie und Ihre Daten könnten ungewollt zum Produkt werden.

▶ Lesen Sie mehr darüber, wie Sie sich sicher online treffen können.

▶ Lesen Sie mehr über die Sicherung privater und betrieblicher Geräte von Mitarbeitenden im Homeoffice (in engl. Sprache).

Schulen Sie Ihre Angestellten und versetzen Sie sich in Ihre Lage

Auch wenn IT für Sie alltäglich ist, ist nicht jeder mit der digitalen Welt vertraut. Versuchen Sie sich in die Lage der einzelnen Beschäftigten Ihres Unternehmens hineinzuversetzen. Wo könnten mögliche Fehlerquellen lauern, was könnte die betreffende Person falsch verstehen, oder wo besteht noch Schulungsbedarf? Veranstalten Sie regelmäßig Schulungen und Workshops zur Cybersicherheit. Stellen Sie außerdem sicher, dass Ihre Mitarbeitenden jederzeit Hilfe erhalten können - eine spezielle E-Mail für anonyme Anfragen ist hier eine gute Lösung.

Führen Sie die Digitalisierung und neue Online-Tools als hilfreiche Komponenten ein, nicht als Pflicht. Wenn Sie Schwierigkeiten haben, etwas zu erklären, oder Ihre Angestellten die Informationen nicht verstehen, versuchen Sie, mit Ihrer Personalabteilung oder Ihren Kommunikationsteams zusammenzuarbeiten, um das Wissen zu vermitteln. Ein kurzer Ausflug in die menschliche Psyche kann helfen. Denken Sie daran, dass es so etwas wie eine dumme Frage nicht gibt.

Versuchen Sie, die Effektivität der Mitarbeitenden pro Aufgabe zu bewerten, nicht pro Stunde. Den größten Anreiz bietet Motivation: Lernen Sie Ihre Beschäftigten gut kennen und finden Sie heraus, welche Art von Aufgaben ihnen Spaß macht. Als interessant empfundene Arbeiten bringen die besten Ergebnisse und eine hohe Produktivität. Zudem werden Kollegen so eher bereit sein, neue digitale Werkzeuge zu nutzen. Und nicht zuletzt sollten Sie das Feedback Ihrer Mitarbeitenden regelmäßig auswerten und sich um ihre Meinungen, Probleme und Ideen kümmern.

Bedenken Sie: Wenn Beschäftigte im Homeoffice arbeiten, neigen sie eher dazu, Informationen aus nicht vertrauenswürdigen Quellen zu lesen und herunterzuladen. Die gewohnte heimische Umgebung verleitet hier leicht zur Sorglosigkeit. Daher sollten ihre Mitarbeitenden wissen, wie sie zwischen normalen und Phishing-E-Mails unterscheiden können. Eine kleine Schulung kann Ihnen auch hier eine Menge Ärger ersparen. Vergessen Sie nicht das schwächste Glied in Ihrer Sicherheitskette: den Faktor Mensch. Angemessene Anweisungen und Schulungen für Mitarbeitende sowohl im Büro als auch im Homeoffice, die möglicherweise von privaten Geräten aus auf kritische Systeme im Unternehmen zugreifen, sollten die Regel werden.

Das Wissen über Malware, Phishing und Co. kann dazu beitragen, einen fahrlässigen Umgang mit den aktuellen Bedrohungen zu verhindern.

Tipp: ▶ ESET-Schulungen zum Thema Cybersicherheit verhindern, dass Ihre Mitarbeiter das Unternehmen gefährden.

So lassen sich verdächtige Informationsquellen erkennen

- Das Veröffentlichungsdatum fehlt
- Der Autor des Artikels fehlt
- Die Online-Verbindung zur Website ist nicht sicher (Schlosssymbol im URL-Feld fehlt – keine HTTPS-Verschlüsselung)
- Der Inhalt ist sehr emotional; es erscheinen viele Ausrufezeichen
- Es wird eine sofortige Handlung gefordert, zum Beispiel etwas zu kaufen oder einige Daten zu teilen
- Der Inhalt ist voller Rechtschreib- und Grammatikfehler und wirkt holperig formuliert
- Textinhalte sind als Grafiken dargestellt

Checkliste zur Erkennung von Phishing-Betrug

- Bewerten Sie die Anfrage. Handelt es sich um eine gewöhnliche oder um eine verdächtige Anfrage?
- Wenn der Absender den Namen eines Mitarbeiters des Unternehmens verwendet, nehmen Sie über einen anderen zuverlässigen Kanal Kontakt mit diesem Kollegen auf. Alternativ schreiben Sie eine neue E-Mail und kontaktieren den Mitarbeiter.
- Akzeptieren Sie keine Dateien und klicken Sie nicht auf irgendwelche Links oder Objekte in E-Mails von Ihnen unbekannten Personen.
- Bevor Sie auf einen Website-Link klicken, versuchen Sie, die Website oder sogar den Namen des Absenders zu googeln, wenn der Name nicht vertraut klingt.
- Senden Sie keine sensiblen Informationen per E-Mail. Melden Sie verdächtige E-Mails immer Ihrer IT-Abteilung.

▶ Erfahren Sie mehr darüber, wie ESET-Lösungen Phishing blockieren.

Fazit: New Work nur mit effizienter und sicherer IT

Kein Zweifel: Die Zukunft der Arbeitsplätze ist digital. Elektronische Prozesse beschleunigen Unternehmensabläufe und helfen Firmen dabei, schnell und flexibel auf immer neue Anforderungen reagieren zu können. Doch New Work verlangt auch nach Sicherheit, damit Unternehmen von den Vorteilen profitieren können.

Cyberbedrohungen werden zunehmen

Die Zahl der Geräte, die online sind, nimmt ständig zu und Tricks von Cyberkriminellen werden immer ausgefeilter, wie beispielsweise der Einsatz hochentwickelter künstlicher Intelligenz zur Verbesserung der Verteilung und Verbreitung von Malware zeigt. Vorbei sind die Zeiten, in denen Phishing-E-Mails sehr leicht zu erkennen waren.

Die Sorgen in Unternehmen vor den Folgen einer Cyberattacke wachsen: Laut einer ▶ Bitkom-Umfrage sind 45 Prozent der Firmen davon überzeugt, dass Cyberattacken ihre geschäftliche Existenz bedrohen können.

Der Gefahr trotzen

Trotz dieser Gefahr wünschen sich immer mehr Menschen Flexibilität am Arbeitsplatz. Dies kann durch die Integration von Online-Lösungen und -Tools erreicht werden, die es den Mitarbeitern ermöglichen, gleichermaßen optimal im Büro, zu Hause oder an einem anderen Ort zu arbeiten.

Ein digitalisierter Arbeitsplatz ermöglicht es Ihnen nicht nur, in Krisenzeiten sicher und produktiv zu bleiben - er trägt auch dazu bei, ein attraktiveres Berufsumfeld gerade für jüngere Fachkräfte zu bieten. Vor allem Arbeitskräften aus der Gruppe der so genannten Millennials (geboren zwischen 1980 und den späten 90er Jahren) und der Generation Z (geboren zwischen den späten 90er und 2010er Jahren), die gerade in den Arbeitsmarkt eintritt, ist das wichtig. Eine von ▶ PwC (PricewaterhouseCoopers GmbH) durchgeführte Untersuchung ergab, dass nicht nur Millennials, sondern alle Generationen von Arbeitnehmern sich mehr Flexibilität und die Option auf Homeoffice wünschen. „Die Ähnlichkeiten in den Einstellungen zwischen den Generationen sind auffällig", heißt es in der Studie. Wenn also digitalisierte Lösungen umgesetzt werden, spricht das Mitarbeitende aller Altersgruppen an und sorgt dafür, dass sie zufriedener, motivierter und produktiver sind. Für dieses Ziel muss ein Rahmen geschaffen werden, der insbesondere den Fokus auf Sicherheit legt. Denn auf diese Weise motivieren New Work und Homeoffice nicht nur die Mitarbeitenden, sondern bringen auf für die Unternehmen den größten Benefit.

ÜBER ESET

Als europäischer Hersteller mit mehr als 30 Jahren Erfahrung bietet ESET ein breites Portfolio an Sicherheitslösungen für jede Unternehmensgröße. Wir schützen betriebssystemübergreifend sämtliche Endpoints und Server mit einer vielfach ausgezeichneten mehrschichtigen Technologie und halten Ihr Netzwerk mit Hilfe von Cloud-Sandboxing frei von Zero-Day-Bedrohungen. Mittels Multi-Faktor-Authentifizierung und zertifizierter Verschlüsselungsprodukte unterstützen wir Sie bei der Umsetzung von Datenschutzbestimmungen.

Unsere XDR-Basis mit Endpoint Detection and Response Lösung, Frühwarnsysteme (bspw. Threat Intelligence) und dedizierte Services ergänzen das Angebot im Hinblick auf Forensik sowie den gezielten Schutz vor Cyberkriminalität und APTs. Dabei setzt ESET nicht nur allein auf Next-Gen-Technologien, sondern kombiniert Erkenntnisse aus der cloudbasierten Reputationsdatenbank ESET LiveGrid® mit Machine Learning und menschlicher Expertise, um Ihnen den besten Schutz zu gewährleisten.

ZUFRIEDENE KUNDEN

BVB 09 Champion Partner

Seit 2019 ein starkes Team
auf dem Feld und digital

Allianz Suisse

Seit 2016 durch ESET geschützt
Mehr als 4.000 Postfächer

ISP Security Partner seit 2008
2 Millionen Kunden

BEWÄHRT

Secur|Ty made in EU
Trust Seal www.teletrust.de/itsmie

ESET wurde das Vertrauenssiegel
„IT Security made in EU" verliehen

CERTIFIED ISO 9001:2015 COMPANY
CERTIFIED ISO 27001:2013 COMPANY

Unsere Lösungen sind nach
Qualitätsstandards zertifiziert

ESET IN ZAHLEN

110+ Mio.
Geschützte Nutzer weltweit

400k+
Geschützte Unternehmen

200+
Länder & Regionen

13
Forschungs- und Entwicklungszentren weltweit

welivesecurity by eset