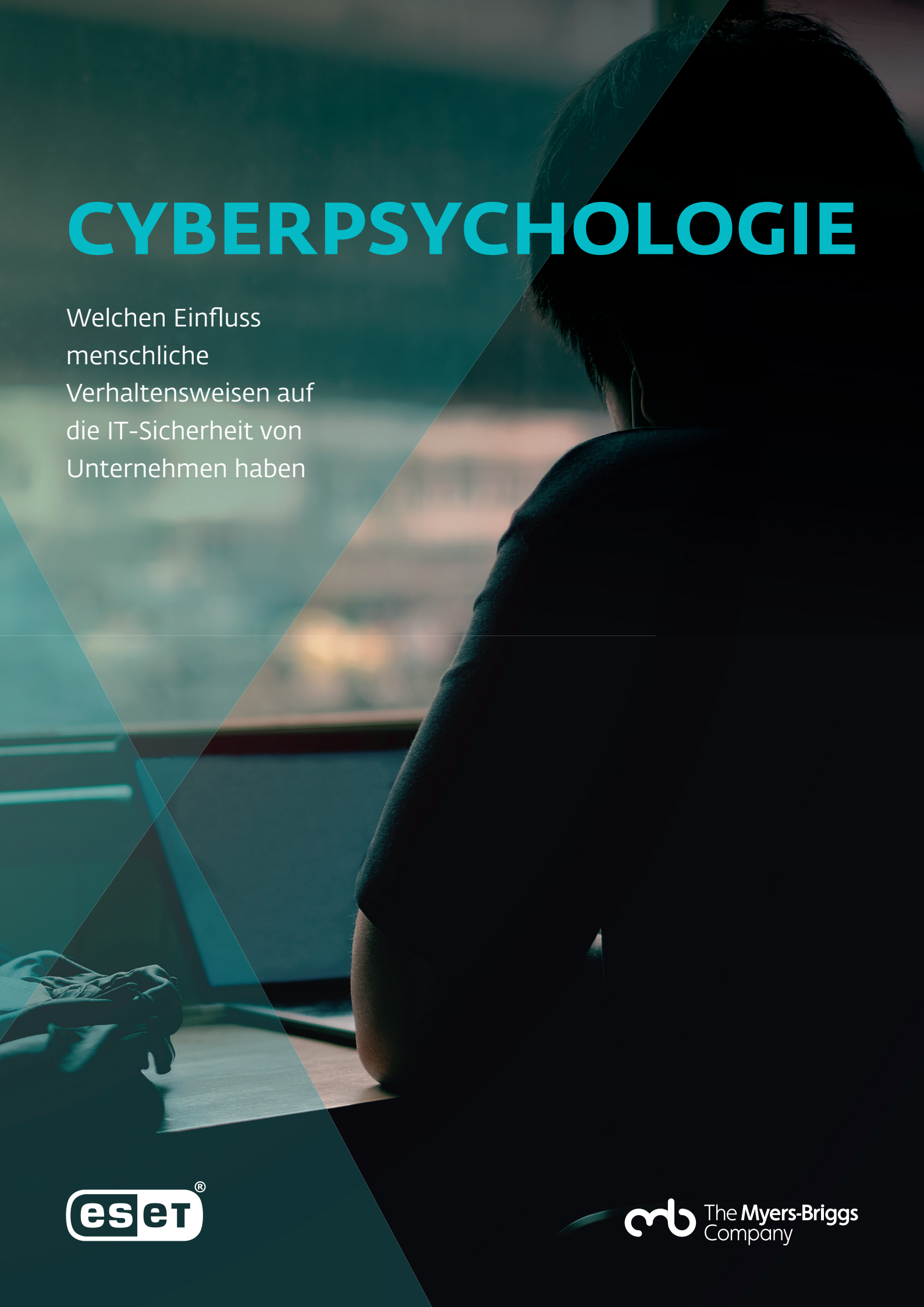


CYBERPSYCHOLOGIE

Welchen Einfluss menschliche Verhaltensweisen auf die IT-Sicherheit von Unternehmen haben

ESET®

The Myers-Briggs Company

IT-Sicherheit ist für Unternehmen so wichtig wie nie zu vor. Die plötzliche Verlagerung der Arbeitswelt ins Home-Office aufgrund der Covid-19 Pandemie zeigt dies noch einmal deutlich. Nur wenige Unternehmen hatten dafür einen Plan B in der Schublade, weder in puncto Equipment noch IT-Security. Zwangsläufig haben die Bereiche Digitalisierung und Datensicherheit einen enormen Schub erhalten. Unternehmen und Mitarbeiter waren und sind dazu gezwungen, sich schnell an die neuen Situationen anzupassen. Nur so können sie den Anforderungen der neuen Realität gerecht werden. In diesem Zusammenhang ist der Druck auf Unternehmen und Mitarbeiter, dynamisch zu agieren und belastbare Strukturen sowie Prozesse zu implementieren, erneut gestiegen. Die IT-Sicherheit eines Unternehmens liegt mehr denn je in den Händen eines jeden Mitarbeiters.

Bereits vor dem Ausbruch von Covid-19 stieg die Anzahl der Cyberangriffe kontinuierlich an. Die Pandemie hat dies noch einmal drastisch verschärft. Vom Betrug per Phishing bis zu Schadprogrammen mit Bezug auf Corona: Der Kreativität von Cyberkriminellen scheinen keine Grenzen gesetzt zu sein. So haben eigene Untersuchungen von ESET ergeben, dass seit Beginn des Lockdowns die Häufigkeit von Cyber-Attacken um 63 Prozent gestiegen ist. Kriminelle nutzen gezielt die abrupten Veränderungen, denen Unternehmen und Mitarbeiter unterworfen sind. Besonders im Fokus stehen dabei die Geräte im Home-Office, an denen die Mitarbeiter ihren Tätigkeiten nachgehen sollen.

ESET deckte in seiner Wirtschaftsstudie „Quo vadis, Unternehmen" kürzlich auf, dass nur knapp 25 Prozent der befragten Firmen Home-Offices optimal ausstatten. Dies führt zwangsläufig dazu, dass Remote Worker ihre Privatrechner einsetzen - in den meisten Fällen weder sicherheitstechnisch professionell administriert noch mit benötigter Software ausgestattet. Oftmals greifen die Mitarbeiter notgedrungen zu fragwürdigen Programmen und Apps. Selbst legitime Antimalwarelösungen findet man längst nicht auf allen Geräten. Dies bedeutet im Klartext: Mangelndes Security-Niveau, ungepatchte Sicherheitslücken sowie unsichere RDP-Verbindungen zwischen Firmenserver und PC laden quasi zum Angriff ein.

Dabei gäbe es ausreichend technische Möglichkeiten, den digitalen Gefahren zu begegnen. Viele Unternehmen sind jedoch aus finanzieller oder technischer Sicht nicht in der Lage, dies zeitnah umzusetzen. So steht der Mitarbeiter mehr denn je „in the line of fire". Zwischen einem Klick auf einen infektiösen Anhang und dem nächsten Sicherheitsvorfall steht dann nur noch der gesunde Menschenverstand – im besten Fall ergänzt um Security-Schulungen. So ist es kein Wunder, wenn das größte Sicherheitsrisiko vor dem Rechner sitzt.

Innerhalb einer ganzheitlichen IT-Sicherheitsstrategie ist es deshalb von zentraler Bedeutung, neben technischen Aspekten auch die individuellen Verhaltensweisen der Mitarbeiter zu berücksichtigen.

Die spannende Frage lautet daher: Welche Rolle spielen Angestellte in puncto IT-Sicherheit für das Unternehmen? Gibt es eine Verbindung zwischen Persönlichkeitstypen und deren Anfälligkeit für Cybercrime?

Um darauf Antworten zu erhalten, ist der Sicherheitssoftwarehersteller ESET eine Kooperation mit dem Unternehmen für Geschäftspsychologie, Myers-Briggs, eigegangen. Für die Analyse wurden über 100 IT-Sicherheitsverantwortliche während der Covid-19 Pandemie befragt und deren Einstellungen und Erfahrungswerte ausgewertet.

Ist der Charakter Gefahr oder Chance für die IT-Sicherheit?

Man liest es in den Medien und hört es von den Experten: Der Mensch ist im Sinne der IT-Security das größte Risiko. Die meisten Sicherheitsvorfälle oder Datenlecks lassen sich tatsächlich auf das Fehlverhalten von Mitarbeitern zurückführen. Die Gründe dafür sind vielfältig: Zu wenig Erfahrung im Umgang mit IT-Security-Fragen und unzureichende Schulungen, aber auch ausgefeilte Angriffe der Cyberkriminellen oder schlichtweg der tägliche Arbeitsstress.

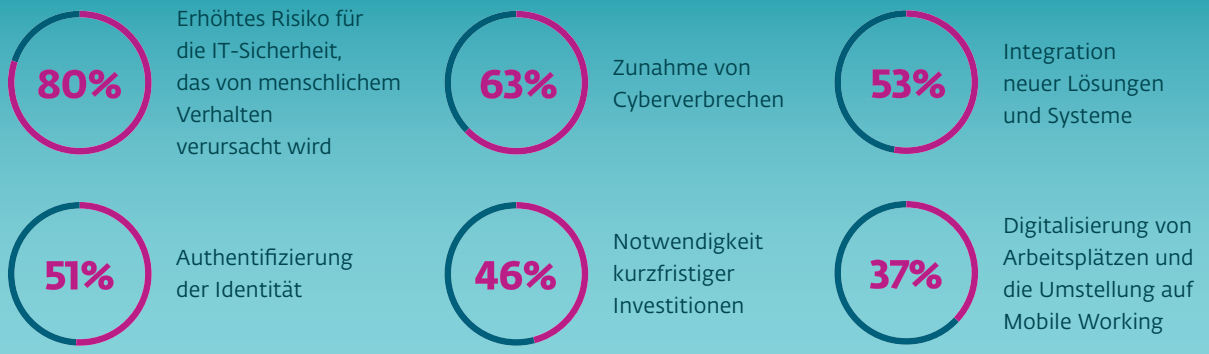
Letzterer betrifft alle Hierarchie-Ebenen, den neuen Praktikanten ebenso wie den (überforderten) IT-Administrator oder die Führungsebene. Die Corona-Krise hat dem Arbeitsleben noch eine Extraschicht Stress und Sorgen aufgetragen. Unter diesen Bedingungen ist es noch schwieriger, weiter konzentriert bei der Arbeit zu sein. Das betrifft vor allem die Remote Worker, die aktuell zwischen Kindergeschrei, Arbeitspensum, Videocalls und Home-Schooling aufgerieben werden. In dem Bericht „Personality and stress in a virtual world" hat Myers-Briggs herausgefunden, dass 47 Prozent der Befragten mehr oder weniger besorgt über ihre Fähigkeit waren, mit Stress während der Corona-Krise umzugehen. So ist es nicht verwunderlich, dass gerade diese Personen anfällig für Cybercrime sind.

Der anhaltende unterbewusste Stress beeinflusst unterschiedliche Persönlichkeitstypen in verschiedener Hinsicht und manifestiert sich in der Art und Weise, wie Menschen in bestimmten Situationen reagieren. Ohnehin gestresste Mitarbeiter könnten eventuell eher in Panik verfallen und auf einen schadhaften Link klicken. Oder ein Mangel an Aufmerksamkeit für Details kann dazu führen, dass eine Sicherheitsverletzung nicht ordnungsgemäß an die IT gemeldet wird.

Wenn menschliches Verhalten ein erhöhtes Risiko für die IT-Sicherheit darstellt, können Unternehmen den Einfluss ihrer Mitarbeiter auf die IT-Sicherheit nicht ignorieren. Wichtiger noch: Gibt es vielleicht sogar Grund-Charaktere, die eher auf Cyber-Angriffe reinfallen als andere? Verstärkt Stress dieses Verhalten oder führt er zu anderen Ausprägungen?

Diese Studie zeigt deshalb auf, wie und warum Personal- und Technik-Abteilungen zusammenarbeiten sollten, um belastbare IT-Systeme, Sicherheitskonzepte und Teams aufzubauen.

Welche zentralen Herausforderungen sehen Unternehmen bei der Einrichtung von Home-Offices?



Der Einfluss von Stress auf Verhaltensweisen

Alltagsstress lässt sich kaum vermeiden. Die Corona-Pandemie hat dafür gesorgt, dass die Anspannung weiter angestiegen ist. In diesem Zusammenhang ist es daher hilfreich, diesen Einfluss auf die eigenen Verhaltensweisen besser zu verstehen - und somit später auch den Umgang mit der IT-Sicherheit.

Der Myers-Briggs Typenindikator (MBTI) gilt als die bekannteste und zuverlässigste Methode zur Persönlichkeitsbeurteilung. Er ermittelt aus unterschiedlichen Charakteristiken einen Persönlichkeitstyp, insgesamt gibt es 16. Sie geben Aufschluss über Art der Interaktionen und der Motivation eines Menschen:

- **Introvert vs. Extrovert (I/E) (Introvertiert vs. Extrovertiert)**
- **Intuition vs. Sensing (N/S) (Intuition vs. sensitives Empfinden)**
- **Feeling vs. Thinking (F/T) (Fühlen vs. Denken)**
- **Judging vs. Perceiving (J/P) (Urteilen vs. Wahrnehmen)**

Der Aktive (ESTP & ESFP)

ESTPs sind meistens analytisch, kontaktfreudig und begeistert sowie logisch. Außerdem sind sie oft aufmerksam und einfallsreich.
ESFP Typen sind meistens tolerant und spontan sowie verspielt und einfallsreich. Außerdem sind sie oft freundlich und begeistert.

Stressfaktoren

- Mangel an Anreizen und Abwechslung
- Theoretisch abstrakte Aufgaben ohne aktuelle, praktische Anwendungen
- Körperliche Eingeschränktheit, z.B. aufgrund von Krankheiten oder anderen Umständen

Verhalten bei alltäglichem Stress

- Suchen mehr und mehr nach externen Anreizen und Abwechslung
- Zeigen ein übermütiges oder gefährliches Verhalten und überschätzen sich
- Manchmal fällt es ihnen schwer, Dinge zu beenden, die sie begonnen haben

Der Entdecker (ENTP & ENFP)

ENTPs sind zumeist aufstrebend, theorieorientiert und anpassungsfähig sowie erfinderisch und provokativ.
ENFPs sind meistens freundlich und ausdrucksstark sowie innovativ und voller Energie.

Stressfaktoren

- Menschen, die sagen: „Es wird nie funktionieren."
- Zu viele „anscheinend" irrelevante Details
- Mangel an Abwechslung, nicht in der Lage zu sein, etwas Neues auszuprobieren

Verhalten bei alltäglichem Stress

- Teilen zunehmend unpraktische Ideen mit anderen Menschen
- Sind unfähig, Dinge ernst zu nehmen, werden destruktiv
- Binden sich nicht an Entscheidungen

Der Einfluss von Stress auf Verhaltensweisen

Der Anführer (ESTJ & ENTJ)

ESTJs sind meistens verantwortungsvoll und effizient, manchmal allerdings auch dominant sowie logisch und realistisch.
ENTJs agieren oft analytisch und provokativ sowie strategisch und hinterfragend.

Stressfaktoren

- Ineffiziente Menschen, Systeme oder Unternehmen
- Mangel an erfolgreichen Abschlüssen bzw. Ergebnissen
- Nicht in der Lage zu sein, Entscheidungen zu treffen
- Sich mehr auf die Gefühle der Menschen fokussieren zu müssen als auf die Aufgaben

Verhalten bei alltäglichem Stress

- Werden zu direkt, energisch, sogar aggressiv
- Treff en vorschnelle Entscheidungen und drängen diese anderen Menschen auf
- Lehnen Beweise/andere Meinungen ab, die nicht zu ihren Sichtweisen passen

Der Emotionale (ESFJ & ENFJ)

ESFJs sind meistens warmherzig und verständnisvoll sowie organisiert, kontaktfreudig und hilfsbereit. Außerdem sind sie realistisch und loyal.
ENFJs sind zumeist warmherzig, kooperativ und unterstützend sowie freundlich und organisiert. Oft bestechen sie darüber hinaus durch ihre hohe Überzeugungskraft.

Stressfaktoren

- Konflikte mit und zwischen anderen Personen
- Mangelnde Herzlichkeit, keine Erwiderung der entgegengebrachten Freundlichkeit
- Ungerechtigkeit im Allgemeinen

Verhalten bei alltäglichem Stress

- Werden überschwänglich und übertrieben freundlich
- Fordern die Erfüllung ihrer Bedürfnisse und die der Anderen ein
- Interpretieren Situationen nach ihren eigenen Werten und ignorieren dabei Fakten

Der Einfluss von Stress auf Verhaltensweisen

Der Bewahrer (ISTJ & ISFJ)

ISTJs sind meistens gründlich, gewissenhaft und realistisch sowie systematisch und zurückhaltend.
ISFJs sind organisiert, praktisch und geduldig sowie zuverlässig und loyal. Außerdem sind sie geduldig und verständnisvoll.

Stressfaktoren

- Ohne detaillierte Informationen oder Pläne agieren zu müssen
- Andere Personen, welche die gemachten Erfahrungen der Bewahrer ablehnen
- Wenn Dinge geändert werden, die schon immer nach einem bestimmten Schema gemacht wurden und funktionieren

Verhalten bei alltäglichem Stress

- Suchen zwanghaft nach vermeintlich wichtigen Informationen
- Ziehen sich vor der Umwelt zurück
- Können keine Entscheidung treffen, bevor nicht alle Informationen zu einem Thema auf dem Tisch liegen

Der Visionär (INTJ & INFJ)

INTJs sind typischerweise strategisch und konzeptionell sowie innovativ, unabhängig und logisch. Außerdem können sie fordernd, aber auch nachdenklich sein.
INFJs sind meistens mitfühlend, idealistisch sowie fantasievoll und visionär. Außerdem sind sie sensibel und zurückhaltend.

Stressfaktoren

- Nicht ausreichend Zeit zu haben, vor der Antwort über alle Möglichkeiten nachzudenken
- Wenn deren wohldurchdachte Ideen abgelehnt oder ignoriert werden
- Unorganisierte, starrsinnige Menschen

Verhalten bei alltäglichem Stress

- Ziehen sich zurück, um komplexere Ideen in ihrem Kopf auszuarbeiten
- Diese Ideen und Modelle könnten weit von der Realität entfernt sein
- Ist unfähig zu handeln, bevor nicht alle Möglichkeiten im Detail untersucht und bewertet wurden

Der Einfluss von Stress auf Verhaltensweisen

Der Analyst (INTP & ISTP)

INTPs sind meistens unabhängig und distanziert. Sie neigen dazu, kritisch und logisch zu sein sowie skeptisch und innovativ.
ISTPs sind meistens analytisch, praktisch und realistisch sowie logisch und anpassungsfähig.

Stressfaktoren

- Wenn ihre sorgfältig abgewogenen Lösungen abgelehnt oder ignoriert werden
- Unlogische Entscheidungen
- Übermäßiges Zeigen von Zustimmung oder Emotionen durch andere Personen

Verhalten bei alltäglichem Stress

- Ziehen sich zurück, um Probleme für sich zu lösen
- Fixieren sich darauf, die eine korrekte Lösung zu finden
- Ignorieren andere Menschen und treffen Entscheidungen, ohne andere Personen darüber zu informieren

Der Gewissenhafte (ISFP & INFP)

ISFPs sind meistens kooperativ, bescheiden und anpassungsfähig sowie sanft und loyal.
INFPs sind zumeist flexibel, spontan sowie nachdenklich und zurückhaltend. Außerdem sind sie fantasievoll und entwicklungsorientiert.

Stressfaktoren

- Menschen, die in einem Job arbeiten, der ihren Werten entgegensteht
- Unflexible und unreflektierte Menschen oder Organisationen

Verhalten bei alltäglichem Stress

- Ziehen sich in einen inneren Dialog zurück
- Arbeiten Entscheidungen zwanghaft durch, um die optimale Lösung zu finden
- Ignorieren Fakten, die nicht in das selbst entworfene Bild passen

Eine Frage der Resilienz

Während wir uns in einem Paradigmenwechsel innerhalb unserer Arbeitswelt und unseres Privatlebens befinden, ist die Widerstandsfähigkeit (Resilienz) wichtiger denn je. Mehr als 50 Prozent der Unternehmen planen, die Änderungen, die während Covid-19 vorgenommen wurden, in irgendeiner Form beizubehalten. Um dies erfolgreich umsetzen zu können, müssen Maßnahmen zum Aufbau widerstandsfähiger IT-Systeme und -Teams ganz oben auf der Agenda der Unternehmen stehen.

Selbstsichere Mitarbeiter, die im Umgang mit IT-Sicherheit geschult sind, bilden die Grundlage einer resilienten IT-Strategie. Wie ESET bei einer Untersuchung zu den Gewohnheiten von 2.000 Angestellten in Großbritannien in puncto IT-Sicherheit herausfand, sorgen sich 68 Prozent der 25–54-Jährigen und 55 Prozent der über 55-Jährigen um die IT-Sicherheit. Auch wenn die Angestellten in der Gruppe der 16-24-Jährigen weniger besorgt waren, bedeutet das nicht zwangsläufig, dass sie ein geringeres Risiko haben, Opfer eines Angriffs zu werden. Denn Selbstüberschätzung sowie fehlende Fähigkeiten und Übungsdefizite der Angestellten können Unternehmen angreifbar machen.

Die überwiegende Zahl von Cyberangriffen ist nicht wegen der Fähigkeiten der Hacker erfolgreich, sondern aufgrund menschlicher Fehler oder Versehen. Tatsächlich gaben 80 Prozent der Unternehmen an, dass eine der größten Herausforderungen während der Corona-Krise die Erhöhung des IT-Sicherheitsrisikos durch den Faktor Mensch war. Die Art und Weise, wie Menschen Informationen konsumieren und kommunizieren, kann eine zentrale Rolle dabei spielen, wie sie an das Thema IT-Sicherheit herangehen. Zudem haben alle Persönlichkeitstypen verschiedene Stärken und blinde Flecken, die sich auf das Ergebnis eines Cyberangriffs auswirken.

Der Myers-Briggs-Typenindikator (MBTI) untersucht wie zuvor beschrieben vier Indikatoren des Persönlichkeitstyps.

- **Extrovertiertheit vs. Introvertiertheit**
- **Intuition vs. sensitives Empfinden**
- **Denken vs. Fühlen**
- **Urteilen vs. Wahrnehmen**

und wie sich diese Bereiche dynamisch verbinden lassen, um die ganze Person zu beschreiben. Zum Beispiel tendieren Menschen mit einem eher extrovertierten Persönlichkeitstyp (Menschen, die kontaktfreudig und vielfältig interessiert sind) dazu, anfälliger für Manipulationen und Täuschungen von Cyberkriminellen zu sein, während Menschen, die beobachten und detailorientiert sind, Phishing-Angriffe besser erkennen und mehr Verständnis für IT-Sicherheitsrisiken haben.

Verschiedene persönliche Präferenzen garantieren jedoch noch keine Erkenntnis oder kein Wissen in puncto IT-Sicherheit. Jedoch kann das Schaffen von Verständnis für die unterschiedlichen Persönlichkeitstypen helfen zu identifizieren, wo individuelle Schwachstellen liegen können.

Mithilfe von psychometrischen Tests und Tools zur Selbstreflektion kann die Personalabteilung dabei helfen, die Zusammensetzung der einzelnen Teams zu erkennen und damit potenzielle Anfälligkeiten genau zu identifizieren. Die IT-Abteilungen können diese Erkenntnisse nutzen, um verständliche Sicherheitsprotokolle zu erstellen und eine proaktive IT-Sicherheitsstrategie zu entwerfen, mit denen man potenziellen Bedrohungen einen Schritt voraus ist.

Persönliche Präferenzen miteinzubeziehen, kann das IT-Sicherheitstraining spannender und effektiver machen – beispielsweise im Zuge umfassender Sicherheitsschulungen während der Einarbeitung oder innerhalb regelmäßiger Wiederholungsschulungen, welche auf die Fähigkeiten der Mitarbeiter zugeschnitten sind. Unter diesen Voraussetzungen ist es wahrscheinlicher, dass Sicherheitsvorschriften eingehalten werden.

Eine Frage der Resilienz

Dies ist besonders vor dem Hintergrund wichtig, dass viele Unternehmen das Home-Office als Arbeitsplatz fest integrieren. Da viele IT-Abteilungen weniger Sichtbarkeit und physischen Zugang zu den einzelnen Mitarbeitern haben, ist es besonders wichtig, sie umfassend weiterzubilden.

Die IT-Sicherheitslandschaft hat sich in den vergangenen zwölf Monaten signifikant verändert, weil Bedrohungen sich gewandelt haben und in neuen Formen wiederaufgetaucht sind. Bösartige Angriffe auf die Unternehmens-IT können vermieden werden, wenn Mitarbeiter ihre eigenen Handlungsmuster kennen und ihnen bewusst ist, für welche Arten von Angriffen sie anfällig sind – und so auf clevere Weise dazu beitragen, die Risiken für die IT-Sicherheit ihrer Organisation effektiv zu minimieren.

Starke Führung für widerstandsfähige Teams

Ähnlich wie das schwächste Glied einer Kette kann ein Mitarbeiter, egal in welcher Position oder Funktion er sich befindet, das Unternehmen in Gefahr bringen. Doch Führungspersönlichkeiten stehen besonders im Visier von Cyberkriminellen: Je höher der Rang oder je wichtiger die Funktion eines Unternehmensmitglieds ist, desto wertvoller wird er für Hacker. Denn diese Person besitzt in der Regel Zugang zu wichtigen Informationen oder mehr Rechte im Netzwerk. Kommt man als Angreifer an dessen Nutzername/Passwort, bieten sich ungeahnte Möglichkeiten.

So verwundert es nicht, dass leitende Angestellte häufiger schwerwiegenden Angriffen ausgesetzt sind, wie etwa durch Spear-Phishing oder Catphishing. Bei diesen zielgerichteten Attacken werden personalisierte Informationen genutzt, um schneller das Vertrauen des potentiellen Opfers zu gewinnen. Ob man Betroffener eines Cyberangriffs wird, hat letztlich weniger mit der Karrierestufe zu tun, sondern vielmehr damit, wie es um das eigene Know-how und Bewusstsein für IT-Sicherheit bestellt ist.

Somit kommt der Führungskraft eine weitere Aufgabe zu: und zwar den Mitarbeitern Sorgfalt beim Umgang und ein Bewusstsein für IT-Sicherheit beizubringen. Dazu zählt selbstverständlich auch, mit sehr gutem Vorbild voranzugehen. Eine kompetente, IT-Security-bewusste Führung ist der Ausgangspunkt für widerstandsfähige Teams in Unternehmen. Damit eine IT-Sicherheitsstrategie effektiv funktioniert, müssen IT-Verhaltensweisen und -Prozesse in die Unternehmenskultur integriert und nicht nur als lästige Aufgabe oder Bürde angesehen werden.

Im vorherigen Kapitel wurde beschrieben, wie sich verschiedene Persönlichkeitstypen unter Stress verhalten. In anderen Untersuchungen hat sich gezeigt, dass unterschiedliche Charaktere nicht nur die Teamdynamik im Allgemeinen beeinflussen, sondern auch das individuelle Verhalten bei Cyberangriffen.

Indem Führungskräfte lernen, ihre eigenen Verhaltensweisen zu reflektieren und zu verstehen, können sie die jeweiligen Handlungen in ihrem Team besser erkennen. Das MBTI-Typen-Modell ist dabei ein effektiver und unkomplizierter Weg, um dies zu tun. Zudem können Führungskräfte, die ihr Verständnis noch weiter vertiefen wollen, auf die Bewertungsmethode MBTI Step II zurückgreifen. Für jede der vier MBTI-Präferenzen betrachtet das Step II-Modell fünf Facetten des Verhaltens, aus denen ein individuelles Bild für jede Persönlichkeit erstellt wird. Beispielsweise werden sich die meisten Menschen mit einer Präferenz zur Extrovertiertheit wohl dabei fühlen, eine Konversation mit einem Fremden zu beginnen. Im Gegensatz dazu werden die meisten Menschen mit einer eher introvertierten Persönlichkeit die Rolle des Beobachters einnehmen. Das Feedback des Step II-Models kann aus diesem Grund besonders für Führungskräfte sinnvoll sein.

Wenn es um IT-Sicherheit geht, ist ein Gespür für die Verhaltensmuster des Teams zu entwickeln genauso wichtig wie die Fähigkeit zur Selbstreflektion. Das Verständnis des Step II-Profils eines Teams hilft, die Schwachstellen im Verhalten zu identifizieren, die Cyberangriffe begünstigen können. Zudem kann es Personal- und IT-Abteilungen helfen, personalisierte IT-Sicherheitsschulungen auf Grundlage der Bedürfnisse des Teams durchzuführen.

Charaktere im Praxis-Check

Wie genau kann das Verständnis der Charaktereigenschaften im IT-Security-Alltag genutzt werden? Am Beispiel von drei unterschiedlichen und aktuellen Bedrohungen können exakte Sicherheitstipps gegeben werden.

Phishing

Phishing-Mails zählen zu den gefährlichsten Angriffsvektoren – und zu den erfolgreichsten. Inzwischen sind die fingierten Nachrichten so täuschend echt gestaltet, dass selbst Experten mehrfach hinschauen müssen, um sie zu entlarven. Insbesondere während der Corona-Pandemie haben Kriminelle massenhaft Spam- und Phishing-Mails mit Bezug zum grassierenden Virus verschickt. Ging es bis zur Mitte des Jahres zunächst um vermeintliche Angebote über Mund-Nasen-Bedeckungen, waren es im vierten Quartal 2020 betrügerische Impfversprechen. Dieses Thema stieg in den E-Mails um rund 50 Prozent an.

Hinter diesen Massenangriffen stehen hochprofessionelle Hacker-Gruppen. Eine der bekanntesten ist die Sednit-Gruppe – auch bekannt als APT28, Fancy Bear, Sofacy oder STRONTIUM – die seit mindestens 2004 operiert und in den vergangenen Jahren Schlagzeilen machte.

Für den Betrug per Phishing scheinen insbesondere die Persönlichkeitstypen empfänglich zu sein, die selbstbewusst, positiv denkend und mutig durch das Leben gehen. Auch enthusiastische und kreative Menschen, denen eine hohe Begeisterungsfähigkeit zugeschrieben wird, müssen besonders vorsichtig sein. Diese Charaktere sollten sich in puncto IT-Sicherheit ausreichend Zeit nehmen, um die Vertrauenswürdigkeit von eingehenden Emails zu überprüfen, bevor sie sie öffnen, Anhänge herunterladen oder die Nachrichten beantworten. Besondere Vorsicht sollten sie bei E-Mails mit interessantem Inhalt oder emotionaler Aufmachung walten lassen.

Charaktere im Praxis-Check

ENFP

- ENFPs gehören zu den ersten, die erkennen, wenn neue Sicherheitsprozesse oder Regeln eingeführt werden.
- Sie nehmen IT-Sicherheit sehr ernst, wenn sie sie als zentralen Wert verinnerlicht haben.

IT-Sicherheitstipps:

- Auch wenn Sie in puncto IT-Sicherheit bereits sehr umsichtig agieren, seien Sie auch oder gerade bei E-Mails misstrauisch, die einen emotionalen Aufmacher beinhalten.
- Wenn Sie sich nicht ganz sicher sind, prüfen Sie den Sachverhalt noch einmal, bevor Sie auf einen Link etc. klicken.

ESTP

- Wenn sie die Relevanz von IT-Sicherheit verinnerlicht haben, erkennen ESTPs Ungereimtheiten schnell.
- Aufgrund ihrer energischen Art und ausgeprägten Problemlösungskompetenz ergreifen sie sofort Maßnahmen.

IT-Sicherheitstipps:

- Seien Sie sich darüber bewusst, das IT-Sicherheit wichtig ist und alle Regeln auch für Sie gelten.
- Beachten Sie die IT-Sicherheitsvorschriften, auch wenn Sie kurzfristig Entscheidungen treffen.

ISTJ

- ISTJs sind aufgrund ihrer gründlichen und gewissenhaften Art gut darin, Diskrepanzen und Fehler in Phishing-Emails zu erkennen.
- Sie nehmen IT-Sicherheit ernst und befolgen die Vorschriften

IT-Sicherheitstipps:

- Auch wenn Sie grundsätzlich sehr auf die IT-Sicherheit bedacht sind, schauen Sie über den Tellerrand hinaus.
- Nutzen Sie keine Varianten desselben Passworts oder identische Passwörter im privaten oder beruflichen Bereich.

ENTP

- IT-affine ENTPs streben danach, kompetent zu wirken und „dumme" Fehler zu vermeiden.
- Sie sind darauf bedacht, die Dinge zum Laufen zu bringen und effizienter zu gestalten.

IT-Sicherheitstipps:

- Nehmen Sie die IT-Sicherheit ohne Ausnahme und in jeder Situation ernst. Dadurch werden Sie andere automatisch als kompetenter ansehen.
- Lesen Sie Emails (auch wenn es schnell gehen muss oder Sie wenig Zeit haben) langsam und aufmerksam durch – Sie könnten etwas bemerken, das Ihnen vorher nicht aufgefallen ist.

ESFP

- ESFPs befolgen im Allgemeinen die IT-Sicherheitsrichtlinien und Vorschriften.
- Aufgrund ihrer Spontanität handeln sie schnell, wenn sie bemerken, dass etwas nicht in Ordnung ist.

IT-Sicherheitstipps:

- Handeln Sie auch in außergewöhnlichen und privaten Situationen vorsichtig. Vertrauen Sie bspw. keinem öffentlichen Netzwerk sensible Daten an, auch nicht dann, wenn es passwortgeschützt ist.
- Nehmen Sie Dinge nicht automatisch als gegeben hin, erst recht nicht dann, wenn Sie Ihnen merkwürdig vorkommen. Seien Sie aufmerksam und bei Bedarf auch misstrauisch.

ISFJ

- ISFJs sind aufgrund ihrer gründlichen und gewissenhaften Eigenschaften gut darin, Diskrepanzen und Fehler in Phishing-Emails zu erkennen.

IT-Sicherheitstipps:

- Handeln Sie auch in außergewöhnlichen und privaten Situationen vorsichtig. Vertrauen Sie bspw. keinem öffentlichen Netzwerk sensible Daten an, auch nicht dann, wenn es passwortgeschützt ist.
- Seien Sie zudem vorsichtig, wem Sie online vertrauen, Cyberkriminelle könnten versuchen, Ihre Gutmütigkeit auszunutzen.

Schadprogramme (Malware)

Malware, auch Malicious Software oder Schadsoftware genannt, zählt zu den größten Risiken für IT-Systeme und Daten. Jeder – ob privat oder dienstlich - der sich im Internet bewegt, kommt zwangsläufig damit in Berührung. Denn die Bandbreite ist riesig und Cyberkriminelle entwickeln pausenlos neue Varianten ihrer erfolgreichsten Angriffswaffe. Insbesondere Ransomware entpuppt sich als besonders lukrativ für Hacker. Anders lassen sich die stetig steigenden Zahlen nicht erklären. Besonders beunruhigend ist die Tatsache, dass Ransomware immer stärker für gezielte Angriffe gegen Unternehmen eingesetzt wird. Das Perfide daran: Kriminelle verschlüsseln nicht nur die Daten ihrer Opfer, sondern drohen bei Nicht-Bezahlung des Lösegeldes mit der Veröffentlichung sensibler Informationen. Dadurch erzeugen sie doppelt Druck auf infizierte Unternehmen.

Persönlichkeitstypen, denen Entscheidungsfreudigkeit, Realitätsnähe und Klarheit zugeschrieben werden, könnten anfälliger für bösartige Downloads sein. Gleiches gilt für Menschen mit ausgeprägtem Organisationstalent und auch diejenigen, die mit eigenwilli-gen oder phantasievollen Arbeitsweisen auff allen.

Während diese Mitarbeiter gewöhnlich das Sicher-heitsprotokoll Schritt für Schritt abarbeiten, könnte dies dazu führen, dass sie um der Effizienz Willen eine schnelle Entscheidung fällen. Abhilfe schafft die strikte Fokussierung auf relevante Informationen, bevor sie Entscheidungen treffen.

Charaktere im Praxis-Check

ESTJ

- ESTJs befolgen in der Regel die IT-Sicherheitsvorschriften und versuchen auch diese zu verbessern.
- Im Allgemeinen nehmen sie Cybersicherheit ernst, jedoch möchten sie dabei auch möglichst effizient arbeiten.

IT-Sicherheitstipps:

- Nutzen Sie nicht die gleichen Passwörter für verschiedene Anwendungen und Systeme.
- Geraten Sie nicht in Versuchung, innerhalb bestimmter Prozesse und Abläufe Abkürzungen zu nehmen, nur weil Sie annehmen, dass Sie dadurch effizienter sein könnten.

ESFJ

- ESFJs sind sich der Relevanz von IT-Sicherheitsrichtlinien bewusst und befolgen sie gewissenhaft.
- Sie eignen sich Verhaltensweisen an, um die IT-Sicherheitsregeln effizient zu befolgen.

IT-Sicherheitstipps:

- Auch wenn Sie sich sicher im Umgang mit IT-Sicherheit fühlen, seien Sie vorsichtig, wem Sie online vertrauen. Beachten Sie die Regeln für IT-Sicherheit auch im privaten Bereich, denn Cyberkriminelle könnten versuchen, Ihr Vertrauen auszunutzen.
- Halten Sie nicht zwanghaft an Dingen und Prozessen fest, nur weil diese schon immer so gemacht wurden. Änderungen der IT-Prozesse werden aus einem bestimmten Grund umgesetzt. Wenn Sie nicht verstehen warum, fragen Sie nach.

INFJ

- INFJs können Dinge überkomplizieren und nach versteckten Bedeutungen suchen.
- Dieses Verhalten kann jedoch ein Vorteil bei der IT-Sicherheit sein.

IT-Sicherheitstipps:

- Wenn sich etwas nicht richtig anfühlt, überprüfen Sie es vorsichtshalber noch ein zweites und drittes Mal.
- Lassen Sie sich nicht davon abbringen, die Details zu überprüfen – Details sind wichtig!

ENTJ

- ENTJs gehören zu denen, die neue Sicherheitsprozesse schnell verstehen und verinnerlichen.
- Sie halten sich auf dem Laufenden und stellen Fragen, um Sicherheitsprobleme zu verstehen und zu erkennen.

IT-Sicherheitstipps:

- Ändern Sie Prozesse und Vorschriften nicht überstürzt, auch nicht, wenn Sie denken, dass Sie damit kurzfristig organisatorische Probleme lösen können.
- Versuchen Sie nicht andere zu überstimmen, weil Sie denken, dass Ihre Lösungsvorschläge effektiver sind. Beziehen Sie auch die Vorschläge anderer in eine Entscheidungsfindung ein.

ENFJ

- ENFJs nehmen IT-Sicherheit ernst, wenn sie sich der Auswirkungen bewusst sind, die die Verstöße gegen die IT- Sicherheitsvorschriften zur Folge haben können.
- Folgen grundsätzlich den IT-Sicherheitsvorschriften, wenn sie klar und verständlich sind.

IT-Sicherheitstipps:

- Seien Sie proaktiv bei der IT-Sicherheit und stellen Sie Fragen, wenn Sie etwas nicht verstehen oder Sie etwas interessiert.
- Verwenden Sie keine Varianten desselben Passworts oder gar identische Passwörter für verschiedene Systeme oder Anwendungen.

INTJ

- INTJs ist es wichtig, über umfassendes Wissen zu verfügen und es laufend zu erweitern. Sie streben danach, fähig und kompetent zu sein.
- Im Allgemeinen befolgen sie IT-Sicherheitsvorschriften.

IT-Sicherheitstipps:

- Sie wissen es nicht zwangsweise am besten, auch nicht, wenn die Regeln für Sie unnötig erscheinen.
- Nehmen Sie die IT-Sicherheit ohne Ausnahme ernst und halten Sie sich auf dem Laufenden. Dies kann Ihnen dabei helfen, dass andere Sie automatisch als fähige und kompetente Person ansehen.

Das Internet der Dinge (IoT)

Das Internet der Dinge (IoT) hat sich längst zum festen Bestandteil unseres Lebens entwickelt: Die Bürotür öffnet sich automatisch beim Ankommen, zum Arbeitsbeginn hat die smarte Kaffeemaschine den Kaffee gekocht und die Schreibtischbeleuchtung passt sich unserer Stimmung an. Und das ruft selbstverständlich Cyberkriminelle auf den Plan, denn viele der eingesetzten IoT-Devices haben Nachholbedarf bei der IT-Sicherheit. Laut dem in Israel ansässigen Sicherheitsunternehmen JSOF sind hunderte Millionen vernetzter Geräte durch 19 Sicherheitslücken für Remote-Angriffe anfällig. Die Fehler, die gemeinsam als Ripple20 bezeichnet werden, betreffen den TCP/IP-Stack des Softwareunternehmens Treck. Zu den gefährdeten Produkten gehören Smart-Home-Geräte, industrielle Steuerungssysteme, medizinische Systeme und Gesundheitssysteme. Außerdem sind Geräte betroffen, die in wichtigen Teilen der Infrastruktur (Energie, Verkehr, Kommunikation) sowie im staatlichen und nationalen Sicherheitssektor eingesetzt werden.

Persönlichkeitstypen, die praktisch veranlagt sind und denen zudem Direktheit sowie Offenheit und Überlegtheit zugeschrieben werden, könnten anfällig sein, wenn sie das Einstellen verbundener Geräte selbst in die Hand nehmen. Auch Menschen mit hoher Problemlösungskompetenz und dem Hang zur Unabhängigkeit sind in Gefahr. Dies gilt auch dann, wenn sie normalerweise die Regeln befolgen. Die beste Herangehensweise für diese Persönlichkeitstypen ist es, nicht immer anzunehmen, man wüsste es am besten. Zudem sollten sie sicherstellen, dass keine Regeln oder Vorschriften ignoriert werden.

Charaktere im Praxis-Check

ISTP

- ISTPs befolgen in der Regel die IT-Sicherheitsvorschriften.
- Besonders für ISTPs ist es jedoch wichtig, dass die Vorschriften einen logischen Sinn ergeben.
- Sie haben grundsätzlich ein gesundes Misstrauen gegenüber Online-Tools und auch anderen Personen im Netz.

IT-Sicherheitstipps:

- Es gibt Gründe für IT-Sicherheitsvorschriften. Wenn sie für Sie unsinnig erscheinen oder Sie sie nicht verstehen, fragen Sie nach.
- Die Dinge schnell und auf die eigene Art tun zu wollen, kann riskant sein. Überlegen Sie in Ruhe, bevor Sie Entscheidungen treffen.

INFP

- INFPs neigen grundsätzlich nicht zu plötzlichen oder riskanten Entscheidungen.
- Sie befolgen in der Regel die IT-Sicherheitsvorschriften. Die Auswirkungen mangelnder IT-Sicherheit zu kennen, hilft INFPs, die Notwendigkeit der Regeln noch besser zu verstehen.

IT-Sicherheitstipps:

- Übernehmen Sie proaktiv Verantwortung für die IT-Sicherheit.
- Nehmen Sie regelmäßige Schulungen und Weiterbildungsangebote in puncto IT-Sicherheit wahr.

INTP

- INTPs interessieren sich für IT-Sicherheit und kennen sich in der Regel mit Fragen in puncto IT-Sicherheit gut aus.
- Sie sind sich der Gefahr von Cyberattacken bewusst und wissen, dass potentiell jeder betroffen sein kann.

IT-Sicherheitstipps:

- Auch wenn Sie möglicherweise skeptisch in Bezug auf neue Regelungen oder Maßnahmen sind, sie wissen es nicht immer am besten! Vorschriften wurden aus bestimmten Gründen festgelegt.
- Wenn Sie etwas nicht verstehen oder skeptisch sind, fragen Sie bei den IT-Experten nach.

ISFP

- ISFPs nehmen die IT-Sicherheitsvorschriften ernst.
- Sie verhalten sich in der Regel sehr sorgfältig und befolgen die Vorschriften detailliert.

IT-Sicherheitstipps:

- Auch wenn Sie bereits sehr umsichtig agieren, warten Sie einen Moment und schauen Sie noch einmal genau hin, auch wenn es gerade hektisch ist.
- Seien Sie zudem vorsichtig, wem Sie online vertrauen. Cyberkriminelle könnten versuchen, Ihre Hilfsbereitschaft auszunutzen.

Zusammenfassung

Unabhängig davon, was die Zukunft bringen wird, zwei Dinge stehen bereits fest: Die Art, wie wir arbeiten, wird sich permanent ändern und Cyberangriff e werden nicht verschwinden. Die Corona-Pandemie hat den Einsatz neuer Technologien in nahezu allen Bereichen beschleunigt. Und aufgrund der Tatsache, dass mehr und mehr Teile unseres Arbeits- und Privatlebens digitalisiert werden, wird IT-Sicherheit der Dreh- und Angelpunkt der Unternehmenssicherheit bleiben.

Cyberangriffe sind eine kontinuierliche Bedrohung für Unternehmen, weswegen sie widerstandsfähige Teams und IT-Systeme aufbauen müssen, um finanzielle und rufschädigende Folgen solcher Attacken zu vermeiden. Das Verständnis von individuellen Persönlichkeiten kann dabei eine Schlüsselrolle in der IT-Sicherheitsstrategie von Unternehmen spielen. So können effektivere Schulungskonzepte entwickelt und Angestellte dazu motiviert werden, sich mehr auf ihre Selbstreflektion und ihre Fähigkeiten zu konzentrieren. Das Verständnis dafür, dass der Faktor Mensch für die IT-Sicherheit genauso wichtig ist wie die technischen Aspekte, ist dabei der erste Schritt, um ganzheitliche IT-Sicherheitskonzepte für Unternehmen zu entwickeln.

In Krisenzeiten hat die Art und Weise der Mitarbeiterführung tiefgreifende Auswirkungen auf die Unternehmenskultur und -moral. Wenn Führungskräfte sich ihrer eigenen Verhaltensweisen und Muster bewusst sind und ihre Teams kennen, können sie Prozesse effektiver vorantreiben und Mitarbeiter auf ihrem Weg zu mehr Selbstreflektion begleiten. IT-Sicherheitskonzepte müssen in allen Unternehmensbereichen tief verwurzelt und fester Bestandteil regelmäßiger Weiterbildungen der Mitarbeiter sein, denn nur damit wird die Basis für die Entwicklung ganzheitlicher IT-Sicherheitsstrategien durch die IT- und Personalabteilungen von Unternehmen ermöglicht.