YEKTA IT

SCHUTZ VOR CYBERANGRIFFEN

KMU LEITFADEN

WHITEPAPER

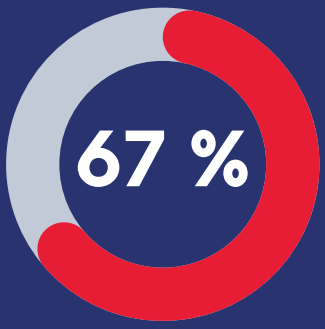
BEST PRACTISES FÜR EFFEKTIVEN SCHUTZ

Herzlich willkommen bei unserem IT-Sicherheits-Whitepaper für KMUs. Hier finden Sie praxisnahe Tipps und Ratschläge, um Ihre digitale Welt sicherer zu gestalten. Verstehen Sie die Bedrohungen und lernen Sie, wie Sie sich und Ihr Unternehmen einfach schützen können.

Yekta IT GmbH, 01.02.2024 - www.yekta-it.de

WIESO DIESES WHITEPAPER EXISTIERT

Cyberkriminalität hat sich für viele KMUs inzwischen zur **größten Bedrohung** entwickelt. Die Frage ist **nicht** mehr o**b**, sondern nur noch wan**n** das eigene Unternehmen betroffen sein wird. Dabei können Unternehmen schon mit geringem Aufwand Ihre Cybersicherheit erheblich erhöhen. Zu diesem Zweck haben wir dieses Whitepaper mit einfach umsetzbaren, **praktischen Tipps** für Sie entwickelt.



der deutschen Unternehmen wurden **Opfer eines Cyberangriffes in 2023** sagt die Studie von Sophos. Falls Sie sich noch nicht ausreichend gewappnet fühlen, dann wird es allerhöchste Zeit sich mit Tipps aus der Praxis für Ihre Cybersicherheit zu beschäftigen.

Über Yekta IT GmbH

Wir sind Familienunternehmen aus Dortmund mit Fokus auf Digitale Transformation & Cybersecurity. Wir stehen für Agilität, Innovation, Fairness und Vertrauen.

Wir verbinden die Werte eines Familienunternehmens mit unserem Anspruch an technologische Exzellenz. Seit Anfang der 2000er folgen wir unserer Mission die Digitalwelt sicherer zu machen.

Cenk Yekta, Geschäftsführer
info@yekta-it.de
+49 231 3981 4905

Die Fakten

Unser Team besteht aus
10 PERSONEN
MIT VIEL LEIDENSCHAFT

Wir haben mehr als
15 JAHRE
ERFAHRUNG IN CYBERSECURITY

Unser Team hat mehr als
20 ZERTIFIZIERUNGEN
WIE OSCP, OSEP, OSWE...

1. IT-Sicherheitsverantwortlichen benennen

Die **wichtigste Rolle** zur Abwehr von Cyberangriffen hat der IT-Sicherheitsverantwortliche. Wenn Sie aktuell niemanden in dieser Rolle haben, ist das die **Priorität Nummer eins!**

Ein kompetenter IT-Sicherheitsverantwortlicher:

- Verfügt über **tiefes Cybersicherheitswissen**.
- Passt **Strategien** an Ihre spezifischen **Bedürfnisse des Unternehmens** an.
- **Identifiziert** und bewertet kontinuierlich **Risiken**.

Wie gehen Sie vor?

- Stellen Sie einen **IT-Sicherheitsverantwortlichen** oder ein Team für IT-Sicherheit auf, um Risiken zu minimieren. Denken Sie auch an Abwesenheitsvertretungen.
- Sorgen Sie dafür, dass dieser genauen **Anforderungen** Ihres **Unternehmens versteht**.
- **Bilden** Sie diesen regelmäßig **weiter**, um auf **neue Bedrohungen reagieren** zu können.

2. Überblick über die IT-Systeme behalten

Sie können sich nur vor Angriffen schützen, wenn Sie wissen, wo Sie angegriffen werden können. Ein guter Überblick ist das Fundament für eine effektive Schutz vor Cyberangriffen.

Warum ist das wichtig?

- **Identifikation von Schwachstellen:** Ein Überblick über Ihre IT-Systeme ermöglicht es, Schwachstellen schnell zu identifizieren und gezielte Maßnahmen zu ergreifen.
- **Effektive Ressourcennutzung:** Durch die Kenntnis Ihrer Systeme können Sie Ressourcen effizienter nutzen, indem Sie veraltete Systeme aussortieren und optimieren.
- **Schnelle Reaktion auf Vorfälle:** Mit einem klaren Überblick können Sie Sicherheitsvorfälle schneller erkennen und angemessen darauf reagieren.

Wie gehen Sie vor?

- **Regelmäßige Inventarisierung:** Führen Sie **regelmäßig** eine **Inventarisierung** Ihrer IT-Systeme durch, um sicherzustellen, dass Sie stets einen aktuellen Überblick haben.
- **Priorisierung der Systeme**: Identifizieren Sie **kritische IT-Systeme** und **priorisieren** Sie deren Dokumentation, da sie besonders wichtig für Ihr Geschäft sind.
- **Verantwortlichkeiten definieren**: Klären Sie, wer für die **Pflege und Aktualisierung** der Dokumentation **verantwortlich** ist, um sicherzustellen, dass sie stets aktuell ist.

3. Regelmäßige Backups durchführen

100% Sicherheit gibt es leider **nie**. Daher gehören zuverlässige **Backups** zu den **wichtigsten Maßnahmen**, um den Geschäftsbetrieb dauerhaft aufrechterhalten zu können.

Wieso ist das wichtig?

- **Geschäftskontinuität gewährleisten:** Regelmäßige **Backups** und **Wiederherstellungs-Tests** sind entscheidend, um im Falle von **Datenverlust** die Geschäftskontinuität sicherzustellen. Dies **minimiert Ausfallzeiten** und hält den Geschäftsbetrieb aufrecht.
- **Finanzielle Verluste reduzieren:** Zuverlässige **Datenwiederherstellung** minimiert Verluste bei Datenverlust oder Ausfallzeiten und **zahlt sich** im Ernstfall **aus**.

Wie sollten Sie vorgehen:

- **Regelmäßige Backups:** Führen Sie **automatisiert & regelmäßig Backups** Ihrer Daten durch, und stellen Sie sicher, dass sie vollständig und korrekt sind.
- **Wiederherstellungs-Tests**: Führen Sie regelmäßige Wiederherstellungs-Tests durch. Sie möchten nicht in einer **Krise** herausfinden, ob die **Backups funktionieren**, oder?
- Wenden Sie die **3-2-1 Regel für Backups** an: 3 Kopien anlegen, mit 2 unterschiedlichen Technologien und 1 davon außerhalb es Büros / Hauses aufbewahren.

---

4. Regelmäßige Updates durchführen

Schnelle Updates können das Risiko von Cyberangriffen erheblich minimieren.

Warum ist das wichtig?

- **Schließung von Sicherheitslücken:** Regelmäßige Updates sind entscheidend, um Sicherheitslücken in Software, Betriebssystemen und Anwendungen zu schließen.
- **Schutz vor Exploits:** Durch regelmäßige Updates wird die Angriffsfläche verringert, da bekannte Sicherheitsprobleme behoben werden, bevor sie ausgenutzt werden können.
- **Gewährleistung der Systemstabilität:** Updates enthalten nicht nur Sicherheitsverbesserungen, sondern auch Fehlerkorrekturen und Verbesserungen.

Wie gehen Sie vor?

- **Automatische Updates aktivieren:** Konfigurieren Sie automatische Updates für Betriebssysteme und Anwendungen, wenn dies möglich ist.
- **Zeitplan für manuelle Updates:** Falls automatische Updates nicht möglich sind, erstellen Sie einen klaren Zeitplan für manuelle Updates.
- **Priorisierung kritischer Systeme:** Identifizieren Sie kritische Systeme und Anwendungen, die besonders geschützt werden müssen, und priorisieren Sie ihre Aktualisierung.

5. Makros managen

Makros in Dokumenten sind ein häufiges Einfallstor für erfolgreiche Cyberangriffe. Daher sollten sie möglich immer deaktiviert werden.

Wie sollten Sie vorgehen:

- **Makros standardmäßig deaktivieren:** Setzen Sie in allen Softwareanwendungen und Richtlinien die Voreinstellung, dass Makros standardmäßig deaktiviert sind.
- **Berechtigungen überprüfen:** Stellen Sie sicher, dass nur wenige und autorisierte Benutzer die Fähigkeit haben, Makros zu aktivieren.
- **Regelmäßige Schulungen:** Sensibilisieren Sie Mitarbeiter für die Risiken von Makro-basierten Angriffen.

GUTER RAT MUSS NICHT TEUER SEIN

oder in diesem Fall überhaupt etwas kosten. Die meisten Tipps, die wir hier für Sie sorgfältig vorbereitet haben, kosten wenig Aufwand, wenig bis gar kein Geld und bieten dafür jede Menge Schutz.

6. Verwenden Sie Virenschutzprogramme

Zuverlässige Virenschutzprogramms gehören zum Standard auf allen Geräten.

Wieso ist das wichtig?

- **Schutz vor Malware:** Ein Virenschutzprogramm erkennt, blockiert schädliche Software wie Malware , einschließlich Viren, Trojanern, Spyware und Ransomware.
- **Sicherung persönlicher Daten:** Ein Virenschutzprogramm schützt persönliche und vertrauliche Daten vor unbefugtem Zugriff.
- **Vermeidung von Systemausfällen:** Ein Virenschutzprogramm minimiert das Risiko von Systemausfällen und sorgt für eine stabilere Betriebsumgebung.

Wie sollten Sie vorgehen:

- Wählen Sie ein gutes **renommiertes Virenschutzprogramm** aus.
- **Regelmäßige Aktualisierungen:** Stellen Sie sicher, dass Ihr Virenschutzprogramm regelmäßig aktualisiert wird und automatisieren Sie diese Aktualisierungen.
- **Regelmäßige Scans durchführen:** Planen Sie regelmäßige Systemscans, um nach Malware zu suchen. Diese Scans können automatisch im Hintergrund laufen.

7. Sichere Passwörter durchsetzen

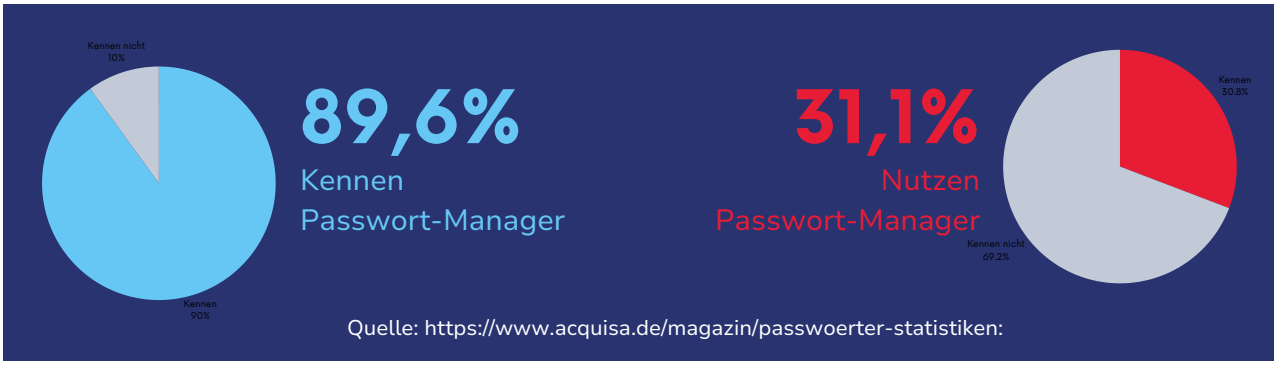
Sichere Passwörter sind wie robuste Schlösser für Ihre Daten. Jedes Teammitglied sollte sich der Bedeutung von sicheren Passwörtern bewusst sein.

Wieso ist das wichtig?

- **Schutz vor Datenverlust:** Sichere Passwörter tragen dazu bei, den Verlust von Daten zu verhindern, sei es in persönlichen Dateien, E-Mails oder anderen Online-Plattformen.
- **Verhinderung von Identitätsdiebstahl:** Starke Passwörter minimieren das Risiko von Identitätsdiebstahl, da sie es erschweren, sich als eine andere Person auszugeben.

Wie sollten Sie vorgehen:

- **Nutzen Sie Passwort-Manager** zur Verwaltung Ihrer Passwörter. Dann müssen sSie sich nur noch wenige Passwörter merken. Diese sollten dann auch komplexer sein.
- Lassen Sie **Passwörter generieren:** Diese sollten Groß- als auch Kleinbuchstaben, Zahlen und Sonderzeichen enthalten. Je länger das Passwort, desto sicherer ist es.
- **Zwei-Faktor-Authentifizierung** aktivieren: Nutzen Sie zwingend die Zwei-Faktor-Authentifizierung, immer wenn verfügbar.



8. Firewall einrichten und konfigurieren

Eine Firewall ist die Schutzbarriere zwischen ihrem internen Netzwerk und dem Internet. Sie überwacht den Datenverkehr, erkennt verdächtige Aktivitäten und blockiert unautorisierte Zugriffe .

Wie sollten Sie vorgehen:

- **Firewall-Software aktivieren:** Stellen Sie sicher, dass die Firewall auf Ihrem Computer oder Netzwerk aktiviert ist und halten Sie diese unbedingt aktuell.
- **Richtige Regel konfigurieren:** Legen Sie klare Regeln für die Firewall fest, um nur den gewünschten Datenverkehr zu erlauben und den restlichen zu blockieren. Sperren Sie ganze Länder, wenn Sie keinen Zugriff von dort erwarten.
- **Regelmäßige Tests durchführen:** Führen Sie regelmäßige Tests und Überprüfungen der Firewall durch. Dies kann bspw. durch Penetrationstests erfolgen.

9. E-Mail Accounts besonders absichern

Der E-Mail Account ist oft die **zentrale Identität** und bietet Zugang zu fast **allen** anderen **Accounts**. Daher sollte dieser besonders **stark abgesichert** werden.

Wie sollten Sie vorgehen:

- **Virenscanner für E-Mails nutzen:** Installieren Sie einen zuverlässigen Virenscanner für E-Mails, um schädliche Anhänge zu identifizieren und zu blockieren. Da E-Mail Accounts oft Einfallstore sind, verhindert dies auch die Verteilung von Malware.
- **Geschäftliche E-Mails geschäftlich behandeln:** Leiten Sie geschäftliche E-Mails nicht auf Ihr persönliches Konto weiter. Geschäftskonten haben höhere Sicherheitsstandards.

10. Unterschiedliche IT-Systeme trennen

Die gezielte Trennung von IT-Systemen hilft, mögliche Angriffspunkte zu minimieren, die Auswirkungen von Sicherheitsverletzungen zu begrenzen.

Wieso ist das wichtig?

- **Begrenzung von Zugriffsrechten:** Durch klare Abgrenzung zwischen normalen Benutzerkonten und Administrator-Konten wird die potenzielle Angriffsfläche reduziert. Dadurch das Risiko von unbefugten Zugriffen und Missbrauch erheblich minimiert.
- **Erfüllung von Compliance-Anforderungen:** In vielen Branchen gibt es Compliance-Anforderungen, die eine klare Trennung von Zugriffsrechten und Konten vorsehen.

Wie sollten Sie vorgehen:

- **Trennung von Benutzer- und Administratorkonten:** Stellen Sie sicher, dass normale Benutzerkonten und Administrator-Konten klar voneinander getrennt sind.
- **Least Privilege-Prinzip anwenden:** Jeder Benutzer sollte nur die minimalen Rechte haben, die für die Ausführung seiner Aufgaben erforderlich sind.
- **Netzwerk segmentieren:** Wenn Sie ein größeres IT-Netzwerk haben, dann isolieren Sie diese voneinander. Nicht jedes System muss mit jedem kommunizieren können.

11. Regelmäßig über IT-Sicherheit informieren

IT-Sicherheit betrifft dauerhaft alle Mitarbeiter des Unternehmens. Daher gehören regelmäßige Informationen und Weiterbildungen zum Pflichtprogramm für alle.

Wie sollten Sie vorgehen:

- Etablieren Sie **klare Kanäle** für die **Informationsübermittlung**, sei es über E-Mails, Intranet, Team-Meetings oder andere Plattformen.
- **Bilden** Sie sich und alle Mitarbeitenden **regelmäßig** zu den aktuellen Best Practises **weiter**. **Sensibilisieren** Sie diese für die **aktuellen Bedrohungen**.
- **Implementieren** Sie **Mechanismen** für die **Notfallkommunikation**, damit kritische Informationen im Notfall schnell verbreitet werden können.

12. Versicherung für Cyber-Risiken abschließen

Viele Unternehmen könnten die Kosten für einen erfolgreichen Cyberangriff nicht alleine stemmen. Genau dafür sind Cyberversicherungen da.

Wieso ist das wichtig?

- **Abdeckung vor finanziellen Verlusten:** Die Cyberversicherung deckt Verluste ab, die durch Cyberangriffe, Datenlecks oder andere Cyber-Risiken entstehen können.
- **Schutz vor Haftungsansprüchen:** Im Falle von Datenschutzverletzungen oder Verlust von Kundendaten können Unternehmen haftbar gemacht werden.
- **Wiederherstellung der Betriebskontinuität:** Die Cyberversicherung kann die Kosten für die Wiederherstellung der Betriebskontinuität und die Behebung von Sicherheitsproblemen abdecken.

Wie sollten Sie vorgehen:

- **Risikobewertung durchführen:** Analysieren Sie die spezifischen Cyber-Risiken, denen Ihr Unternehmen ausgesetzt ist und bewerten Sie, welche Sie absichern möchten.
- **Auswahl der geeigneten Cyberversicherung:** Wählen Sie eine Cyberversicherung, die zu den spezifischen Bedürfnissen und Risiken Ihres Unternehmens passt.
- **Aktualisierung der Cyberversicherung:** Überprüfen Sie regelmäßig Ihre Cyberversicherung, um sich den ändernden Risiken und Bedürfnissen anzupassen.

13. Risiken der mobilen Arbeit managen

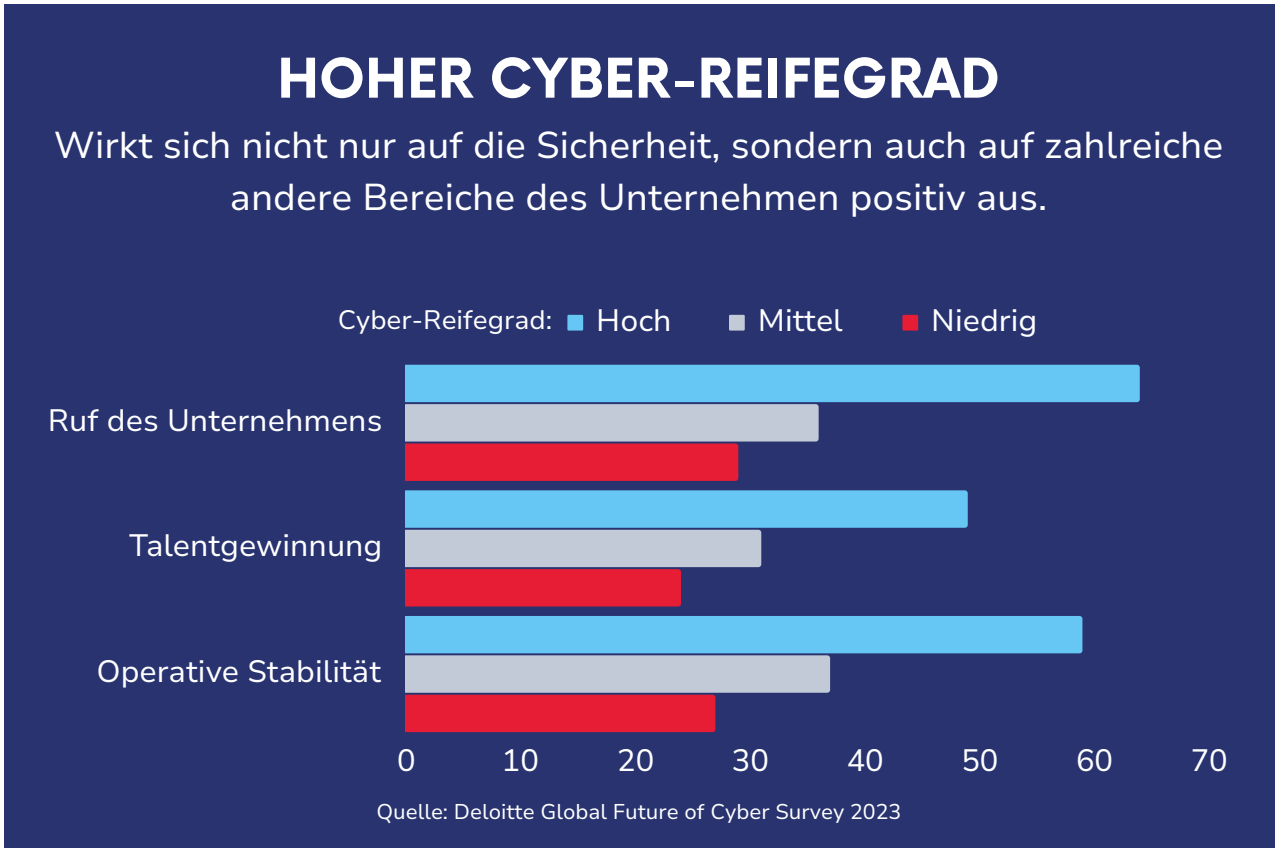
Home Office sowie mobiles Arbeiten sind aus unserem Alltag nicht mehr wegzudenken. Damit gehen zahlreiche neue Risiken einher, die es zu managen gilt.

Wieso ist das wichtig?

- **Schutz von Unternehmensdaten:** Homeoffice und Geschäftsreisen erfordern den Zugriff auf sensible Unternehmensdaten von verschiedenen Standorten aus. Diese Daten vor sind unbefugtem Zugriff und potenziellen Datenschutzverletzungen zu schützen.
- **Einhaltung von Datenschutzbestimmungen:** Unternehmen müssen geltende Datenschutzbestimmungen einhalten, unabhängig davon, wo die Mitarbeiter arbeiten.
- **Wahrung des intellektuellen Eigentums:** Viele Unternehmen haben wertvolles intellektuelles Eigentum, welches vor Diebstahl oder Verlust zu schützen ist, um Wettbewerbsvorteile zu erhalten und Innovationen zu schützen.

Wie sollten Sie vorgehen:

- **VPN nutzen**: Ermutigen Sie alle Mitarbeiter dazu, ein Virtual Private Network (VPN) zu verwenden, um eine sichere Verbindung zum Unternehmensnetzwerk herzustellen.
- **Regelmäßige Schulungen:** Sensibilisieren Sie Mitarbeiter für die spezifischen IT-Risiken im Homeoffice und während Geschäftsreisen.
- **Zwei-Faktor-Authentifizierung:** Implementieren Sie die Zwei-Faktor-Authentifizierung, um die Zugangssicherheit zu erhöhen.



14. Incident Response Plan entwickeln

Kommt es trotz aller Maßnahmen zu einem erfolgreichen Cyberangriff, ist eine schnelle und effektive Reaktion entscheidend, um den Schaden zu minimieren.

Wieso ist das wichtig?

- **Schadensbegrenzung:** Eine schnelle Reaktion hilft, den Schaden zu begrenzen und eine weitere Ausbreitung des Angriffs zu verhindern.
- **Schutz von Daten:** Eine prompte Reaktion kann Datenschutzverletzungen verhindern und die Integrität kritischer Informationen zu bewahren.
- **Vertrauenswürdigkeit aufrechterhalten:** Eine transparente und angemessene Reaktion hält das Vertrauen von Kunden, Partnern und anderen Stakeholdern aufrecht.

Wie sollten Sie vorgehen:

- **Alarmierung des IT-Sicherheitsteams:** Informieren Sie unverzüglich das IT-Sicherheitsteam, um den Vorfall effektiv bewältigen können.
- **Sofortige Erkennung und Isolierung:** Identifizieren Sie den Angriff so früh wie möglich und isolieren Sie betroffene Systeme, um eine weitere Ausbreitung zu verhindern.
- **Benachrichtigung relevanter Stakeholder:** Informieren Sie interne Teams, Geschäftsführung, Kunden und über den Vorfall und die getroffenen Maßnahmen.
- **Zusammenarbeit mit Behörden:** Melden Sie den Vorfall ggf. den entsprechenden Behörden, um rechtlichen Anforderungen zu entsprechen.
- **Post-Incident-Analyse:** Führen Sie eine umfassende Nachanalyse durch, um aus dem Vorfall zu lernen und zukünftige Sicherheitsvorkehrungen zu verbessern.

In diesem Whitepaper haben wir für Sie die wichtigsten Handlungsempfehlungen zusammengetragen, um Ihr Unternehmen vor Cyberangriffen zu schützen. Diese Tipps orientieren sich an den besten Standards und basieren auf unserer langjährigen Erfahrung. Wir hoffen, dass diese für Sie genauso nützlich sind, wie viele Unternehmen, die wir bereits beraten durften.

Haben Sie noch Fragen rund um IT-Sicherheit oder möchten Sie unsere kostenlose Erstberatung in Anspruch nehmen? Dann sind wir gerne für Sie da.

info@yekta-it.de
+49 231 3981 4905

Cenk Yekta
CEO

Ali Recai Yekta
CTO & Head of Cybersecurity