
Security.
Cyber-Risiken
in der Schweiz.
#zukunftsstark
Ihr starker IT-Partner.
Heute und morgen.
BECHTLE

Inhaltsverzeichnis

Die Bedrohung ist real.

Die Digitalisierung ist aus praktisch keiner Branche mehr wegzudenken. Mit der zunehmenden Bedeutung von IT und Cloud Computing für immer mehr Geschäftsprozesse und der allgegenwärtigen Vernetzung der Systeme werden auch die Risiken und Bedrohungen aus dem Cyberspace immer relevanter: Hacker und andere Cyberkriminelle, Geheimdienste und weitere staatliche und private Akteure nutzen das Internet für ihr ureigenen Zwecke und verursachen erheblichen Schaden – vom Abgreifen finanzrelevanter und persönlicher Daten über Industriespionage bis zum vollständigen Lahmlegen des Betriebs. Die Methoden der Angreifer werden dabei immer zahlreicher, raffinierter und automatisierter.

- So zeigt die Studie «Clarity on Cyber Security» von KPMG[1] von Mitte 2018, dass von den befragten Schweizer Unternehmen, aufgrund einer Cyberattacke, 42% einen finanziellen Schaden erlitten, 42% einen Ausfall von kritischen Geschäftsprozessen verzeichneten und 25% einen spürbaren Reputationsschaden hinnehmen mussten.

- Bezüglich der Entwicklung von Malware – Viren, Würmer, Trojaner & Co. – stellt zum Beispiel der «Bedrohungsbericht Februar 2019» von Cisco[2] fest, dass Malware wie Emotet die Bedrohungslandschaft weiter dominieren und meistens immer noch über Email Verbreitung finden.

- Kein Wunder, dass auch das World Economic Forum die Bedeutung der Cyber-Bedrohungen erkannt hat: Im «Global Risks Report 2018» des WEF[3] figurieren erstmals Cyberattacken in den Top-5 der Risiken. Im «Global Risks Report 2020» des WEF[4] befinden sich Cyberattacken immer noch in den Top-10 der Risiken, zusammen mit Datenklau und Datenbetrug und befinden sie sich damit in der gleichen Kategorie wie Naturkatastrophen und Klimawandel. Das World Economic Forum sieht die Cyber-Bedrohung auch als wesentliches Risiko über die nächsten zehn Jahre.

Die zitierte KMPG-Studie weist jedoch auch nach, dass Schweizer Unternehmen noch nicht genügend vorbereitet sind. Zwar haben 82 Prozent der befragten Firmen einen Massnahmenplan zur Abwehr von Cyberattacken, beziehen aber Angriffe auf ihre Zulieferkette und Geschäftspartner nicht mit ein. Das Problem ist real und betrifft die Privatwirtschaft, sowie auch die öffentliche Hand. Anfangs 2020, wurde der Schweizer Autoimporteur AMAG das Ziel eines Cyberangriffs[5], welcher Auswirkungen auf die Ersatzteilversorgung der nachgelagerten Betriebe zur Folge hatte.

Mit der steigenden Zahl und Komplexität der Angriffe wird eines klar: Die klassische Firewall genügt nicht mehr, um den Cyber-Risiken zu begegnen. IT-Sicherheit ist zur strategischen Frage geworden, die im Unternehmen einen zentralen Platz einnehmen sollte. Mit einem sorgfältig geplanten Sicherheitskonzept auf Basis einer eingehenden Risikoanalyse lässt sich das Problem jedoch eingrenzen und beherrschen. Dabei helfen neben modernen Sicherheitslösungen oder cloudbasierten Security-Plattformen, auch ein aktuelles Informationssicherheits-Managementsystem (ISMS) und Sensibilisierungs-Trainings für Mitarbeiter.

1 https://assets.kpmg/content/dam/kpmg/ch/pdf/clarity-on-cyber-security-2018.pdf
2 https://www.cisco.com/c/de_ch/products/security/security-reports.html
3 https://www.weforum.org/reports/the-global-risks-report-2018
4 https://www.weforum.org/reports/the-global-risks-report-2020
5 https://www.luzernerzeitung.ch/news-service/wirtschaft/amag-von-hackern-angegriffen-ld.1190701

Die aktuellen Top-Bedrohungen für die Schweiz.

In der Schweiz analysiert die Meldestelle Analyse und Informationssicherung des Bundes (MELANI) laufend die Cyber-Bedrohungslage. Der aktuelle Halbjahresbericht 2019/II[6] zeigt die konkreten Hauptbedrohungen für Juli bis Dezember 2019:

- Cyber-Spionage
- Angriffe auf IoT-Geräte und industrielle Kontrollsysteme
- DDoS-Attacken
- Social Engineering und Phishing
- Datenabflüsse
- Ransomware

In seinem ersten Bericht zur Bedrohungslage gemäss dem neuen Nachrichtendienstgesetz[7] weist auch der Bundesrat Anfang Mai 2019 darauf hin, dass zur Spionage zusammen mit traditionellen Methoden oft Cybermittel eingesetzt werden. Im Fokus stehen demnach Behörden, die internationalen Organisationen in Genf, Diplomaten und diplomatische Vertretungen, Unternehmen aus dem Technologie-, Rüstungs- und Finanz- und Handelssektor sowie die Hochschulen.

Eine hohe Bedeutung misst der Bericht zudem Angriffen auf kritische Infrastrukturen zu. Mehrere Bundesstellen und Privatfirmen seien bereits Opfer ausländischer Cyberangriffe geworden, die hohen Schaden angerichtet hätten. Der Energiesektor stehe im Moment vermehrt im Fokus von Spionage- und Aufklärungskampagnen. Im Ausland habe es gezielte Sabotageaktionen auf die Stromversorgung bereits gegeben (Ukraine 2016), und die Ransomware WannaCry habe die Notfallsysteme der Spitäler in Grossbritannien erheblich beeinträchtigt. Das Fazit des Berichts: «Je häufiger solche Cyberangriffe werden, desto grösser ist das Risiko, dass die Schweiz und ihre kritischen Infrastrukturen zumindest Kollateralschäden erleiden.»

6 https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2019-2.html
7 https://www.vbs.admin.ch/content/vbs-internet/de/ueber-das-vbs/organisation-des-vbs/die-verwaltungseinheiten-des-vbs/-der-nachrichtendienst-des-bundes.detail.nsb.html/74905.html

Cyber-Spionage.

Ob sie von Staaten oder Unternehmen ausgeht: Spionage, das gezielte Abgreifen von Informationen aus machtpolitischen Gründen oder um Geschäftsgeheimnisse zu erlangen, spielt sich zunehmend im Cyberspace ab. Angreifer nutzen dazu technische Schwachstellen in IT-Systemen und Netzwerken aus – und sie versuchen, mittels Social-Engineering-Methoden wie Phishing und Spear-Phishing an die Zugangsdaten berechtigter Nutzer zu kommen und auf dieser Basis in die Informationssysteme einzudringen. Die technische Sicherheit ist zwar Grundvoraussetzung für die Abwehr von Spionageattacken, der Faktor Mensch spielt jedoch eine mindestens so wichtige Rolle.

EMPFEHLUNG:

- Wissen, was wertvoll ist: Klassifizieren Sie die in den IT-Systemen gespeicherten Informationen und schützen Sie besonders wertvolle Daten durch Massnahmen wie Verschlüsselung.
- Lassen Sie allen involvierten Mitarbeitenden ein umfassendes Sicherheitstraining zukommen, insbesondere was Social Engineering, wie Phishing, etc. und den Umgang mit sensiblen Daten, wie Zugangsdaten, Personendaten, etc. betrifft.

BEISPIEL:

Angreifer versandten gezielte Phishing-E-Mails, die beim Aufruf der angehängten Dokumente die Schadsoftware «Olympic Destroyer» freisetzten. Die Adressaten waren Finanzorganisationen in Russland und Laboratorien im Bereich der Gefahrenabwehr. Eine Variante dieser E-Mails kam in Form einer gefälschten Einladung zu einer internationalen Konferenz daher, die angeblich vom Bundesamt für Bevölkerungsschutz und vom Labor Spiez stammte. Das Labor selbst wurde dabei nicht angegriffen, es wurde lediglich missbraucht, um der Einladung mehr Seriosität zu verleihen.

Angriffe auf IoT-Geräte und industrielle Kontrollsysteme.

Sowohl MELANI als auch der NDB sehen das Internet der Dinge (IoT) als neuen Brennpunkt der Cybersicherheit. Denn viele Geräte, die mit dem Internet verbunden sind, bieten wenig oder gar keinen Schutz vor Cyberangriffen und können sehr leicht ausgespäht, sabotiert oder so manipuliert werden, dass sie falsche Daten übermitteln. Und sie können gekapert, zu einem Botnetz zusammengefasst und zum Beispiel für DDoS-Attacken missbraucht werden, um andere Systeme lahmzulegen. Dies gilt auch für industrielle Kontrollsysteme, die ursprünglich nicht für die Vernetzung konzipiert waren und später ins IoT integriert wurden.

Das IoT stellt die IT-Sicherheit vor diverse Herausforderungen. So ist es bei manchen IoT-Devices gar nicht möglich, Sicherheitsfunktionen auf dem Gerät zu integrieren. Und die Hersteller beheben Schwachstellen gar nicht oder nur zögerlich. Auch in Unternehmen kommen zudem vielfach IoT-Geräte zum Einsatz, die eigentlich für den Privatgebrauch konzipiert sind und nicht über das erforderliche Sicherheitsniveau verfügen. Dazu kommt, dass die vorhandenen IT-Sicherheitslösungen IoT-Geräte oft nicht erfassen. Viele Unternehmen wissen deshalb überhaupt nicht genau, welche IoT-Devices wo installiert sind.

EMPFEHLUNG:

- Visibilität ist unabdingbar: Erstellen Sie ein Inventar aller vernetzten Systeme – bis hin zum einzelnen IoT-Gerät.
- Beachten Sie auch private Geräte, die von den Mitarbeitenden ins Firmennetzwerk gebracht werden.
- Nutzen Sie eine IT-Sicherheitslösung, die auch IoT-Geräte berücksichtigt.
- Machen Sie Gebrauch vom «Minimalstandard zur Stärkung der IKT-Resilienz»[8], der vom Bundesamt für wirtschaftliche Landesversorgung (BWL) herausgegeben wurde.
- Beachten Sie auch die Checkliste «Massnahmen zum Schutz von Industriellen Kontrollsystemen»[9].

BEISPIEL:

Die Gemeinde Ebikon stellte eines Tages fest, dass Angreifer mehrere tausendmal versuchten, ins Netzwerk der autonomen Betriebssteuerung der Wasserversorgung einzudringen. Die Versuche blieben glücklicherweise erfolglos, und Ebikon konnte die bereits getroffenen Sicherheitsmassnahmen weiter justieren, um künftig noch besser gerüstet zu sein.

8 https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html
9 https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/massnahmen-zum-schutz-von-industriellen-kontrollsystemen--ics-.html

DDoS-Attacken.

Eine DDoS-Attacke (Distributed Denial of Service) hat zum Ziel, die Verfügbarkeit eines IT-Systems durch Überflutung mit Anfragen einzuschränken oder das System ganz lahmzulegen. Angriffsziele sind oft Websites oder Online-Shops – somit kann eine DDoS-Attacke direkt Umsatzverluste zur Folge haben oder den Ruf eines Unternehmens tangieren, weil der Webauftritt nicht erreichbar ist.

Für Angriffe dieser Art kommen oft so genannte Botnetze zum Einsatz: IT-Systeme oder IoT-Geräte zahlreicher Nutzer und Unternehmen werden gekapert und für das Absenden der Massenanfragen missbraucht. Die missbrauchten Absender merken meist nichts davon. Die Angriffe auf die Zielsysteme erfolgen auf unterschiedlichen Ebenen: Standen traditionell Netzwerk und Systemressourcen im Fokus (Layer 3 und 4), zielen die Angreifer zunehmend auch auf die Anwendungsebene ab (Layer 7) und überlasten die auf den Systemen laufenden Applikationen direkt.

EMPFEHLUNG:

- Überwachen Sie den Netzwerkverkehr kontinuierlich mit einem IDS-System (Intrusion Detection), um Anomalien sofort zu erkennen, wie sie bei einer DDoS-Attacke auftreten.
- Nutzen Sie eine Web Application Firewall, um die Angriffsfläche Ihrer webbasierten Dienste zu minimieren.
- Konfigurieren Sie die Firewall so, dass nur die wirklich benötigten Protokolle auf das jeweilige System Zugriff haben.
- Weitere Empfehlungen zur Abwehr von DDoS-Attacken finden Sie im MELANI-Dokument «Massnahmen gegen DDoS-Attacken»[10].

BEISPIEL:

Die Hackergruppe «Apophis Squad» bekannte sich zu zahlreichen DDoS-Attacken, darunter einen Angriff auf den Schweizer Secure-E-Mail-Provider Protonmail, der den Dienst tagelang beeinträchtigte. Am Ende stand die Verhaftung der Mitglieder der Hackergruppe. Danach gab es jedoch weitere Erpressungsversuche unter dem Namen „Apophis Squad", die aber von Trittbrettfahrern stammten, die auf den Fall Protonmail hinwiesen und mit heftigen DDoS-Attacken drohten. Passiert ist am angekündigten Datum jedoch nichts.

10 https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/massnahmen-gegen-ddos-attacken.html

Social Engineering und Phishing.

Social Engineering zielt auf den Faktor Mensch ab. Angreifer versuchen an vertrauliche personen- oder unternehmensbezogene Daten heranzukommen oder die Systeme der Betroffenen mit Schadsoftware zu infizieren und nutzen dabei die unterschiedlichsten Methoden von Fake-Anrufen bis zu E-Mails mit der Aufforderung, Passwörter, Konto- oder Kreditkartendaten zwecks Verifizierung über einen im E-Mail platzierten Link in ein gefälschtes Online-Formular einzutragen. Im Fall von solchen E-Mails spricht man von Phishing. Waren Phishing-Mails früher rasch an schlechtem Deutsch oder amateurhafter grafischer Umsetzung zu erkennen, haben die Angreifer aufgeholt und präsentieren immer echter wirkende Fake-Nachrichten mit Bezug zu realen Begebenheiten.

Eine spezielle, vermehrt aufkommende Variante ist das Spear-Phishing: Dabei zielen die Angreifer nicht willkürlich auf eine breite Masse von Adressaten ab, sondern gezielt auf konkrete Organisationen und Personen. Die Empfänger werden dazu im Vorfeld sorgfältig recherchiert, zum Beispiel auf Social-Media-Plattformen, und die Angreifer geben sich als Geschäftspartner, Vorgesetzte oder anderweitig vertrauenswürdige Absender aus. Der Inhalt der E-Mails kann auf Basis der Recherchen ganz auf den einzelnen Empfänger zugeschnitten werden.

EMPFEHLUNG:

- Geben Sie niemals per Telefon, E-Mail oder in einem Webformular persönliche Zugangsdaten weiter.
- Installieren Sie niemals Software oder folgen einem Link, wenn Sie per Telefon oder E-Mail dazu aufgefordert werden.
- Prüfen Sie kritisch, wenn sich jemand mit einem ungewohnten Anliegen an Sie wendet und nehmen Sie Rücksprache.
- Regeln Sie als Unternehmen sämtliche Prozesse, die den Zahlungsverkehr betreffen klar und präzise und halten Sie die Mitarbeitenden an, sich konsequent nach den Regeln zu richten.
- Lassen Sie allen involvierten Mitarbeitenden ein umfassendes Sicherheitstraining zukommen, insbesondere was Social Engineering, Phishing-Mails und den Umgang mit Zugangsdaten betrifft.

BEISPIELE:

MELANI wurden eine Reihe von Anrufen gemeldet, bei denen sich die Anrufer als Mitarbeitende einer Bank ausgaben und um die Ausführung eines «E-Banking-Update» baten. Dazu sollte jeweils eine Remote-Control-Software wie TeamViewer installiert und danach unter Eingabe der E-Banking-Zugangsdaten der Firma eine Testzahlung ausgeführt werden. Währenddessen haben die Angreifer Fernzugriff auf das System, können die Eingaben abgreifen und eigene Zahlungen auslösen.

Office 365 wird zum Ziel von Cyberkriminellen. Per Phishing-Email fordern sie ihre Opfer zur Eingabe der Office-365-Zugangsdaten auf. Typischerweise ist der Office-365-Zugang nur mit einer User-ID in Form der Email-Adresse und mit einem Passwort abgesichert. Danach schreiten sie zum so genannten Überweisungsbetrug: Sie suchen in den betroffenen Office-365-Accounts nach elektronischen Rechnungen und stellen sie mit einer anderen IBAN nochmals zu. Solche Angriffe zielen vor allem auf Firmen ab, die grosse Rechnungen an ausländische Empfänger ausstellen. Ein Angreifer im Besitz der Zugangsdaten des CEO einer Firma konnte so den Finanzchef zu einer dringenden Überweisung von einer Million US-Dollar bewegen – er selbst könne die Zahlung nicht auslösen, da er in einem Meeting festsitze. Dies war tatsächlich der Fall, und der Angreifer hatte dank Zugriff auf den Kalender des CEO Kenntnis davon.

E-Banking-Trojaner.

Unter Crimeware versteht man Schadsoftware, die gezielt kriminellen Aktionen dient. So etwa zur Sabotage von IT-Systemen, zur Manipulation von Daten, zur Spionage oder zum Massenversand von Spam-Mails. Ein weiteres Ziel von Crimeware ist die Finanzindustrie, und dabei besonders der Zahlungsverkehr per Online- oder Offline-E-Banking. Im Jahr 2018 war «Retefe» wiederum einer der bedeutendsten E-Banking-Trojaner in der Schweiz, der auf Windows- und MacOS-Systeme von Privatanwendern zielt und über manipulierte Word-Dokumente auf die Systeme der Opfer gelangt. Ist das Zielsystem infiziert, können sich die Angreifer in den E-Banking-Prozess einklinken und Überweisungen umleiten.

Ein weiterer oft vorkommender E-Banking-Trojaner namens Gozi nimmt auch Offline-Payment-Systeme und damit Unternehmen ins Visier, die eher solche Systeme als direktes Online-E-Banking nutzen. Trojaner sind allerdings nicht mehr der einzige Mechanismus, mit dem Kriminelle die Banking-Informationen ihrer Opfer sammeln. Vermehrt finden sich in offiziellen und inoffiziellen App-Stores gefälschte vorgeblich von Banken stammende Apps, in die man Kreditkarten- oder Login-Informationen eingeben soll, um beispielsweise die Kreditlimite zu erhöhen.

EMPFEHLUNG:

- Verwenden Sie für Zahlungen dedizierte Geräte mit eingeschränktem Internetzugang. Diese Geräte sollten für keine anderen Internet-Aktivitäten wie E-Mail-Abruf oder Surfen genutzt und immer mit den aktuellen Sicherheitsupdates versorgt werden.
- Setzen Sie für die Freigabe von Zahlungen auf das Vier-Augen-Prinzip und führen Sie die Freigabe auf einem zweiten Gerät durch.
- Seien Sie vorsichtig bei Anhängen insbesondere im Word-Format und öffnen sie ein Attachment nur, wenn der Absender klar identifiziert und vertrauenswürdig ist.

BEISPIEL:

Die PostFinance war von einer Fake-App betroffen. Die gefälschte App im PostFinance-Erscheinungsbild fragte nach Kreditkartendaten. Nachdem der Nutzer diese Daten eingegeben hatte, erschien bloss eine «Danke»-Seite und die App wurde beendet – höchste Zeit, die Kreditkartenfirma zu kontaktieren und die Karte sperren zu lassen.

Ransomware.

Ransomware – auch Cryptolocker oder Erpressungstrojaner genannt – ist eine Kategorie von Crimeware, die schon manchem Unternehmen direkten Schaden zugefügt hat, von der Ein-Personen-Firma bis zum Kantonsspital. Laut Medienberichten häufen sich Ransomware-Angriffe seit Anfang 2019 erneut. Ransomware verschlüsselt die Daten der Opfer, sodass sie nicht mehr lesbar sind. Dies kann die Geschäftstätigkeit komplett zum Erliegen bringen. Erst gegen Übermittlung eines bestimmten Betrags in Form von Kryptowährungen wie Bitcoin werden die Daten wieder entschlüsselt – angeblich, denn es ist keineswegs sicher, dass wirklich entschlüsselt wird, wenn man auf die Erpressung eingeht.

Für MELANI gehört Ransomware nach wie vor zu den Angriffsarten mit den grössten Auswirkungen für KMU sowie für kritische Infrastrukturen. Am verbreitetsten sind zurzeit die Ransomware-Varianten Ryuk, GandCrab, Dharma und Locky. Besonders auffallend ist Ryuk: Die Ransomware sammelt im Vorfeld Daten und verschlüsselt auf dieser Grundlage gezielt Systeme von ergiebigen Opfern. Zur Verbreitung nutzt Ryuk den Trojaner Emotet, der über Social Engineering und gefälschte E-Mails mit angehängtem Word-Dokument eingeschleust wird. Emotet war ursprünglich als Banking-Trojaner konzipiert, dient heute jedoch vornehmlich dem Spamversand und dem Nachladen zusätzlicher Malware. Im Fall von Ryuk lädt Emotet zunächst die Malware Trickbot nach, die das ganze Netzwerk abgrast und sich so selbstständig weiterverbreitet. Erst wenn so ein genügend grosses Netzwerk erkannt wurde, wird die eigentliche Ransomware nachgeladen – sonst wäre der Angriff für die Täter wohl zu wenig lukrativ.

EMPFEHLUNG:

- Damit die Verschlüsselung nicht zum Problem wird, erstellen Sie regelmässig ein Backup Ihrer Daten und lagern Sie dieses auf einem externen Medium, das Sie nach der Sicherung vom System trennen oder auf einem Cloudspeicher, der nicht automatisch synchronisiert wird. So gehen Sie sicher, dass im Ransomware-Fall nicht auch das Backup verschlüsselt wird.
- Setzen Sie Sicherheitslösungen ein, die den Zugriff auf die Daten nur zugelassenen Applikationen erlauben.
- Segmentieren Sie das Netzwerk und trennen Sie so gefährdete Bereiche ab, die oft E-Mails von unbekannten Absendern öffnen müssen. Die Ransomware kann sich dann nicht auf andere Segmente fortpflanzen.

IT-Sicherheit mit Bechtle Schweiz AG.

Bechtle kennt die Herausforderungen der IT-Sicherheit – sowohl was die technische Sicherheit betrifft als auch bei der Informationssicherheit und beim Datenschutz. Aus der Erfahrung mit Sicherheitsproblemen und Lösungen ist die «360-Grad-Lösung» Bechtle Security entstanden, die alle Aspekte der IT-Sicherheit End-to-End abdeckt. Sie besteht aus verschiedenen Modulen eines Security Operation Centers und gewährleistet, dass Bedrohungen rechtzeitig erkannt und behoben werden, noch bevor sie sich auf das Unternehmen auswirken könnten.

Bechtle Security bietet folgende Komponenten und Vorteile:

- Beratung, Implementierung, Analyse und Betrieb aus einer Hand
- Umfassendes Sicherheitskonzept
- Betriebsunterstützung vor Ort im Rahmen eines Onsite-Betriebes
- Security-Monitoring, Log-Analyse, Cyber Defense und Threat Intelligence
- Remote-Betrieb von Security-Infrastrukturen oder in Teilen
- Security Incident Management oder als integrierte Leistung im Rahmen eines IT Incident Managements
- Kooperationen und Partner-Zertifizierungen mit allen namhaften Security-Herstellern
- Höchste Beratungskompetenz dank Competence Center Bechtle Internet Security & Services (BISS) in Neckarsulm mit über 150 Security Engineers und Consultants

IT-Sicherheit beginnt mit der Beratung. Wir beraten Sie umfassend zu allen IT-Sicherheitsthemen:

- Application Security
- Cloud Security
- Cyber Crime & Defense
- Datacenter Security
- Datenschutz und Informationssicherheit
- Security Awareness Training
- Infrastruktur- und Perimeter-Security
- Workplace Security

Damit Sie die Sicherheitslösung erhalten, die zu Ihrem Unternehmen passt, erarbeiten wir alles von Anfang an und unterstützen Sie tatkräftig bei der Umsetzung:

- Analyse des Sicherheitsbedarfs
- Konzeption und Erstellung eines Proof of Concept
- Implementierung der Sicherheitslösungen in der Infrastruktur durch unsere zertifizierten Sicherheitsexperten
- Know-how und Wissenstransfer dank unseres Competence Centers Bechtle Internet Security & Services (BISS)
- Cyber Crime & Defense

BECHTLE SCHWEIZ AG.

Als ein führender IT-Dienstleister der Schweiz sind wir, Bechtle Schweiz AG, für KMU, Grosskunden und öffentliche Institutionen der Partner erster Wahl für Consulting, IT-Infrastruktur, Cloud-Lösungen, IT-Services und Software. Unser Angebot umfasst von der Beratung über die Umsetzung bis zum Betrieb den gesamten IT-Life-Cycle. Unsere Kunden profitieren von höchsten Partnerzertifizierungen bei den meisten namhaften Herstellern. Mit über 600 Mitarbeitern an neun Standorten sind wir für unsere Kunden ein zuverlässiger und nachhaltiger Partner, der sie in sämtlichen Belangen der IT mit Kompetenz und Erfahrung unterstützt.

10 STANDORTE.

- Baar
- Basel
- Bern
- Carouge
- Mägenwil
- Morges
- Pratteln
- Regensdorf
- Rotkreuz
- St.Gallen

BECHTLE GRUPPE CH.

- Abissa, abissa.ch
- Acommit, acommit.ch
- Alpha Solutions, alphasolutions.ch
- ARP, arp.ch
- Bechtle Schweiz, bechtle.ch
- Bechtle direct, bechtle.ch
- Codalis, codalis.ch
- Solid Solutions, solidsolutions.ch

BECHTLE INTERNATIONAL.

- 1983 in Neckarsulm (DE) gegründet
- 75 IT-Systemhäuser in der DACH-Region
- 24 E-Commerce-Gesellschaften in 14 Ländern
- Über 11.000 Mitarbeiter
- Mehr als 70.000 Kunden
- Bechtle ist im MDAX und im TecDAX notiert
- 2018 lag der Umsatz bei rund 4,3 Milliarden Euro

Mehr auf: bechtle.ch

Bechtle Schweiz AG
Telefon +41 848 820 420
info.ch@bechtle.com | bechtle.ch

Baar | Basel | Bern | Carouge | Mägenwil | Morges | Pratteln | Regensdorf | Rotkreuz | St.Gallen

Ihr starker IT-Partner.
Heute und morgen.

BECHTLE