MediaMarktSaturn Business

Cyberangriffe kennen, verstehen und vermeiden

Cyberangriffe können Unternehmen empfindlich treffen – Datenverlust, Reputationsschäden und finanzielle Einbußen sind keine Seltenheit. Um sich zu schützen, hilft es, die Techniken der Kriminellen zu kennen. Wir geben Ihnen einen Überblick, welche Arten von Cyberattacken es gibt und wie sich Schäden vermeiden lassen.

Was ist ein Cyberangriff?

Ein Cyberangriff (häufig auch: Hackerangriff) bezeichnet eine bösartige Handlung, die darauf abzielt, Computersysteme, Netzwerke, oder Daten zu schädigen, zu manipulieren oder zu stehlen. Solche Angriffe können von Einzelpersonen, organisierten Hackergruppen oder auch staatlich geförderten Akteuren durchgeführt werden. Ziel eines Cyberangriffs ist es häufig, sensible Informationen zu stehlen, Unternehmen finanziellen Schaden zuzufügen oder deren Geschäftsbetrieb zu stören.

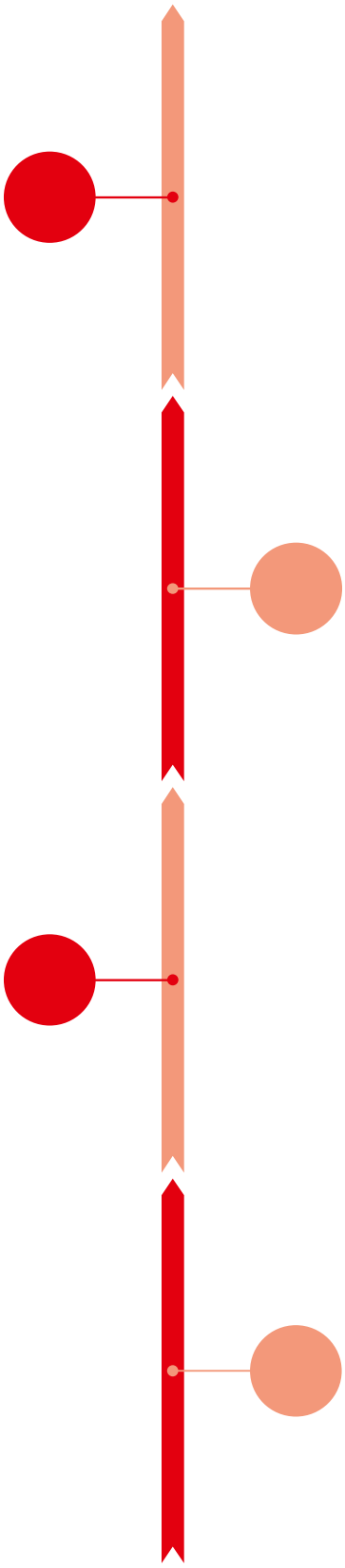
Arten von Cyberangriffen

Es gibt verschiedene Arten und Formen von Cyberangriffen. Nicht alle zielen dabei auf die Sicherheitssysteme Ihrer IT-Infrastruktur. Zu den häufigsten und erfolgreichsten Methoden gehört das Ausnutzen der „Schwachstelle Mensch“. Einige der wichtigsten Hackerangriffe stellen wir im Folgenden vor:

Arten von Cyberangriffen

Phishing

Methode, bei der Angreifer böswillige E-Mails, Websites oder Nachrichten verwenden, um vertrauliche Informationen wie Passwörter, Kreditkartennummern oder andere sensible Daten zu stehlen. Diese Angriffe basieren auf sozialer Manipulation: Sie wollen entweder Vertrauen gewinnen oder die betroffenen unter Druck setzen, damit die potenziellen Opfer Ihre Daten freiwillig auf gefälschten Websites eingeben und so den Hackern zur Verfügung stellen.



Spoofing

Technik, bei der Angreifer eine vertrauenswürdige Identität vortäuschen, indem sie E-Mails, IP-Adressen oder Telefonnummern fälschen. Ziel ist es, Vertrauen zu erschleichen und darüber Sicherheitsmaßnahmen zu umgehen. Ein bekanntes Beispiel ist der Enkeltrick. Im Unternehmensumfeld könnte sich ein Angreifer etwa als Mitarbeiter des IT-Supports ausgeben und versuchen, so an Passwörter und andere sensible Daten zu gelangen.

Social Engineering

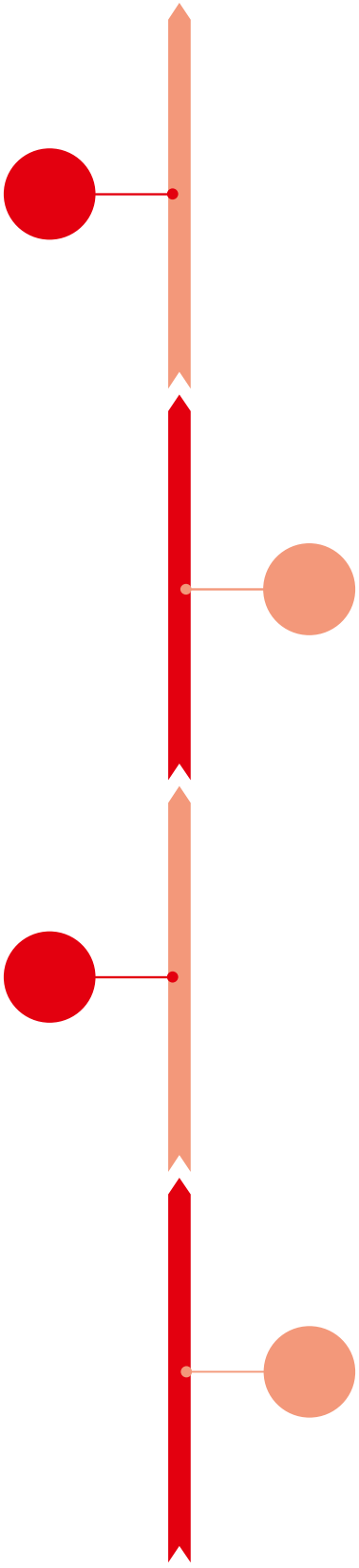
psychologische Manipulationstechniken, um Personen dazu zu bringen, vertrauliche Informationen preiszugeben oder Sicherheitsbarrieren zu umgehen. Angreifer nutzen dabei gezielt menschliche Eigenschaften wie Vertrauen, Hilfsbereitschaft, Respekt vor Autoritäten oder Angst, um Personen zu manipulieren. Diese Techniken kommen unter anderem beim Phishing und Spoofing zum Einsatz.

Malware

bezeichnet Schadsoftware wie Trojaner, Viren, Würmer und Ransomware. Sie werden oft über infizierte Anhänge oder Downloads verbreitet und können erhebliche Schäden anrichten, indem sie Daten zerstören, Systeme lahmlegen oder Informationen stehlen.

Ransomware

Form von Malware, die in Systeme eindringt und Daten – oder das ganze System – verschlüsselt und dadurch für den Benutzer unzugänglich macht. Besonders gefährlich: Auch Backups können gezielt attackiert werden. Die Angreifer nehmen Ihre Daten als Geisel und fordern in der Regel ein Lösegeld (engl.: ransom), um den Zugriff wiederherzustellen.



Trojaner

Art von Malware, die sich als nützliches Programm tarnt, um Benutzer dazu zu verleiten, sie auszuführen. Sobald der Trojaner aktiv ist, kann er – je nach Programmierung – verschiedene Aufgaben ausführen. Unter anderem können Trojaner Hintertüren öffnen, um Angreifern Zugriff auf ein System zu gewähren, weitere Schadsoftware installieren, Tastatureingaben aufzeichnen, gezielt sensible Daten stehlen oder das infizierte Gerät zum Teil eines Netzwerks für DDoS-Angriffe machen.

DDoS-Angriffe

Steht für Distributed-Denial-of-Service-(DDoS)-Angriff. Überlastet ein System oder eine Website mit einer großen Anzahl von Anfragen, sodass legitime Benutzer keinen Zugriff mehr haben. Solche Angriffe können den Betrieb eines Unternehmens erheblich beeinträchtigen. Häufig werden sie auch als Ablenkung von weiteren Angriffen oder zur Vorbereitung von Folgeattacken genutzt.

SQL-Injection

Hier schleusen Angreifer bösartigen Code per Datenbankabfragen ein, um unautorisierten Zugriff auf Datenbanken zu erhalten. Diese Form des Angriffs zielt darauf ab, sensible Informationen wie Kundendaten oder Finanzinformationen zu stehlen, zu manipulieren oder zu löschen. SQL (Structured Query Language) ist eine Standardsprache für die Kommunikation mit relationalen Datenbanken. SQL-Datenbanken kommen häufig für Webanwendungen oder Websites zum Einsatz, was sie zu einem beliebten Ziel von Cyberkriminellen macht.

Schäden durch Cyberangriffe

Die Auswirkungen von Cyberangriffen auf Unternehmen sind vielfältig und oft verheerend. Laut Bitkom-Studie betrug der Schaden, den deutsche Unternehmen im Jahr 2024 durch Cyberangriffe erlitten, 178,6 Milliarden Euro. Die häufigsten Angriffsformen sind laut dem Branchenverband Ransomware-Angriffe und Phishing. Zu den häufigsten Schäden gehören:

Direkte Kosten durch Diebstahl, Lösegeldzahlungen oder Betriebsunterbrechungen können enorm sein.

Ein Datenleck oder ein Angriff kann das Vertrauen von Kunden und Partnern erheblich beeinträchtigen und zu Abwanderungen führen.

Datenschutzverletzungen können zu hohen Strafen führen, insbesondere unter Gesetzen wie der DSGVO.

Ausfallzeiten oder eingeschränkte Systeme können den Geschäftsbetrieb erheblich behindern.

Unternehmen sind häufig Ziele von Cyberangriffen

Unternehmen sind für Cyberkriminelle besonders attraktive Ziele, da sie wertvolle Daten wie Kundeninformationen, Finanzdaten oder geistiges Eigentum besitzen. Besonders kleine und mittelständische Unternehmen (KMU) sind gefährdet, da sie häufig über weniger ausgefeilte Sicherheitsmaßnahmen verfügen. Daher ist es besonders wichtig, bereits während der Digitalisierung Ihres Unternehmens einen professionellen IT-Check durchzuführen.

Große Unternehmen hingegen stehen im Fokus gezielter Angriffe, die mit erheblichem Aufwand geplant werden.

Laut e-Crime-Studie der KMPG haben Angriffe auf Mobilgeräte stark zugenommen. Während Sie im Jahr 2022 noch 7 Prozent der Angriffe ausmachten, waren es 2024 bereits beunruhigende 27 Prozent. Schutz können ein gutes Mobile Device Management (MDM) oder in die Hardware integrierte Sicherheitsvorrichtungen wie Samsung Knox bieten.

Gut zu wissen: Moderne IT-Hardware ist oftmals bereits mit integrierten Lösungen ausgestattet, die das Sicherheitsrisiko minimieren. Ihr MediaMarktSaturn Business Kontakt berät Sie gerne umfassend und herstellerunabhängig.

So können Sie Ihr Unternehmen schützen

Der Schutz vor Cyberangriffen erfordert eine Kombination aus technologischen Lösungen, Schulungen und klaren Richtlinien. Die besten Softwaresicherungen nützen wenig, wenn die Angestellten etwa Phishing nicht erkennen und dadurch Angriffsflächen schaffen. Wichtige Maßnahmen sind:

01 Schulungen der Belegschaft

Sensibilisieren Sie Ihr Team regelmäßig für potenzielle Gefahren wie Phishing-E-Mails oder verdächtige Anhänge.

02 Regelmäßige Software-Updates

Halten Sie Betriebssysteme und Anwendungen stets auf dem neuesten Stand, um Sicherheitslücken zu schließen.

03 Verwendung von Firewalls und Antivirenprogrammen

Schützen Sie Ihre Netzwerke und Geräte mit professionellen Sicherheitslösungen.

04 Sichere Backups erstellen

Regelmäßige Datensicherungen stellen sicher, dass Sie im Falle eines Angriffs schnell wieder handlungsfähig sind.

05 Starke Passwörter, Multi-Faktor-Authentifizierung, Passkeys

Erschweren Sie unbefugten Zugriff durch den Einsatz komplexer Sicherheitsverfahren.

06 Sicherheitsaudits durchführen

Lassen Sie Ihre Systeme regelmäßig von Experten überprüfen, um Schwachstellen zu identifizieren.

Mehr Informationen zum Thema Sicherheit finden Sie in unserem Artikel Schutz vor Cyberattacken.

Überblick: Cyberangriffe erkennen und abwehren

Unternehmen geraten zunehmend unter Druck, Ihre IT abzusichern. Die Zahl der Hackerangriffe und Schäden steigen jährlich weiter an. Besonders Angriffe wie Phishing, die den Faktor Mensch ins Visier nehmen, werden immer häufiger. Daher ist es empfehlenswert, die Belegschaft regelmäßig zu schulen. Gegen Angriffe mit Malware helfen in der Regel technische Lösungen, die Schadsoftware erkennen und unschädlich machen.

Ein starker Schutz vor Cyberangriffen erfordert also ein Zusammenspiel aus präventiven Maßnahmen, technischer Ausstattung und der Sensibilisierung aller Beteiligten. Indem Unternehmen die Bedrohungen ernst nehmen und proaktiv handeln, können sie Risiken minimieren und im Ernstfall schnell reagieren.

Finden Sie passende Lösungen und Ihren persönlichen Ansprechpartner:

mediamarkt.de/de/b2b-registration;
saturn.de/de/b2b-registration

Ansprechpartner

Stefan Köstler
Head of National Sales

Per Mail:
geschaeftskunden.vertrieb@mediamarkt.de
vertrieb.business@saturn.de

Sie suchen IT-Lösungen aus einer Hand? Als Europas größter Fachhändler für Elektronikprodukte unterstützen wir Ihr Business mit einem persönlichen Ansprechpartner, einem riesigen Sortiment und unabhängiger Beratung. Ganz egal, ob Solo-Selbstständig, KMU oder Großunternehmen, ob Start-Up, öffentliche Verwaltung oder Gastrobetrieb: Als Geschäftskunde von MediaMarktSaturn machen Sie mehr aus Ihrem Business.

MediaMarktSaturn Business

MediaMarkt SATURN