FORUM

Cyber Security

präsentiert von MORGENSTERN

MORGENSTERN

Whitepaper

Cyber Security

Inhalt

Wir bei MORGENSTERN legen großen Wert auf inklusive Sprache. Deswegen gendern wir – und zwar gerne! Du sollst dich von unseren Texten angesprochen fühlen, egal wer du bist.

Fachbegriffe gendern wir jedoch nicht, da sie wie Eigennamen feststehende Begriffe sind. Hier geht es nicht um das generische Maskulinum, sondern um fachliches Vokabular, das seine eigene juristische Bedeutung hat.

...dir aber nun **viel Spaß**, liebe*r Leser*in!

01. Einführung

In Zeiten der Digitalisierung nimmt die Bedeutung der Cyber Security für Organisationen immer weiter zu. Cyberangriffe sind eine Bedrohung, der jede Organisation unabhängig, von ihrer Größe, ausgesetzt ist.

Die Gründe dafür sind vielfältig: Zum einen steigt die Anzahl der vernetzten Geräte in Organisationen stetig an, zum anderen werden Cyberkriminelle immer raffinierter und nutzen immer ausgefeiltere Methoden, um in Netzwerke einzudringen. Daher ist es von entscheidender Bedeutung, dass Organisationen angemessene Maßnahmen ergreifen, um ihre Daten und Systeme zu schützen.

In diesem Whitepaper geht es darum, dich für das Thema Cyber Security zu sensibilisieren, aufzuzeigen was die typischen Einfallstore und Angriffsmethoden sind und welche Kosten und Folgen ein Cyberangriff mit sich bringen kann. Des Weiteren wird auf die rechtlichen Pflichten für Organisationen eingegangen und darauf, welche Maßnahmen zu treffen sind, um die Cybersicherheit zu erhöhen.

Brauchst du Rat? Kontaktiere uns! Wir bei MORGENSTERN haben ein erfahrenes und hoch spezialisiertes Team bestehend aus Anwälten & Anwältinnen, Datenschutz- und IT-Sicherheitsexpert*innen!

contact@morgenstern-privacy.com
+49 (0) 6232 - 100119 44

Mehr MORGENSTERN Whitepaper findest du übrigens auch unter:
morgenstern-privacy.com & morgenstern-legal.com

02. Was verbirgt sich hinter dem Begriff "Cyber Security"

Cyber Security (dt. Cybersicherheit) ist ein ständig wachsendes und sich entwickelndes Thema, da immer mehr Aspekte unseres täglichen Lebens von Informationstechnologie abhängen. Es bezieht sich auf die Praktiken, Technologien und Prozesse, die verwendet werden, um Computer, Netzwerke, Software und elektronische Daten vor unbefugtem Zugriff, Diebstahl, Beschädigung oder Missbrauch zu schützen. Es geht darum, Risiken im Zusammenhang mit der Verwendung von Informationstechnologie zu identifizieren, zu bewerten und zu minimieren. Dies soll die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Systemen gewährleisten. Zu den wichtigsten Aspekten der Cyber Security gehören die Identifizierung von Schwachstellen, die Implementierung von Sicherheitsmaßnahmen, die Schulung von Mitarbeiter*innen zur Vermeidung von Bedrohungen durch soziale Technik und das schnelle Erkennen und Reagieren auf Sicherheitsverletzungen.

Jahrelang konzentrierten sich die Bemühungen im Bereich der Cyber Security auf den Schutz eines Netzwerks vor externen Angriffen, aber die Mitarbeiter*innen arbeiten heutzutage vermehrt dezentral und nutzen ihre persönlichen Geräte für die Arbeit oder arbeiten mit den geschäftlichen Geräten im Homeoffice.

Aus diesem Grund spielt der menschliche Faktor eine sehr entscheidende Rolle bei der Cyber Security. Menschen können zum Beispiel Opfer von Angriffen werden, indem man versucht durch das Abfangen von Passwörtern oder anderen sensiblen Informationen Zugang zu Systemen oder Daten zu erhalten. Die meisten Sicherheitsverletzungen werden durch menschliches Versagen verursacht, entweder durch fahrlässiges Verhalten oder durch Absicht.

Das hat zur Folge, dass Cyberkriminelle ihre Angriffe von technischen Schwachstellen auf menschliche verlagern und somit die Mitarbeitenden zur Zielscheibe werden!

03. Zahlen, Daten und Fakten zu Cyberattacken und den verursachten Schäden

Cyberangriffe haben in den letzten Jahren dramatisch zugenommen und verursachen immense wirtschaftliche Schäden weltweit. Folgende Zahlen, Daten und Fakten zu Cyberattacken verdeutlichen das Problem:

- Laut einem Bericht des Cybersecurity Ventures hat der weltweite Schaden durch Cybercrime im Jahr 2021 6 Billionen US-Dollar erreichen.
- Im Jahr 2020 gab es weltweit mehr als 304 Millionen Malware-Attacken, was einem Anstieg von 13,7% im Vergleich zum Vorjahr entspricht.
- Im Jahr 2020 wurden mehr als 100 Milliarden Angriffe auf das Internet der Dinge (IoT) durchgeführt, was einem Anstieg von 300% gegenüber dem Vorjahr entspricht.
- Phishing ist nach wie vor eine der häufigsten Cyberangriffsmethoden. Laut einem Bericht der Anti-Phishing Working Group wurden im ersten Quartal 2021 weltweit mehr als 222.000 Phishing-Angriffe gemeldet.

- Ransomware ist eine der verheerendsten Cyberangriffsmethoden, da sie Daten verschlüsselt und Lösegeld erpresst. Laut einem Bericht von Coveware stieg das durchschnittliche Lösegeld im Jahr 2020 auf 233.817 US-Dollar.

https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

- Die Top-Branchen, die am meisten von Cyberangriffen betroffen sind, sind laut einem Bericht von Verizon die Finanzdienstleistungsbranche, der Gesundheitssektor und der öffentliche Sektor.

- Laut dem Bericht des Ponemon Institute zum "Cost of a Data Breach" betrug der durchschnittliche Schaden durch einen Datenverstoß im Jahr 2020 3,86 Millionen US-Dollar.

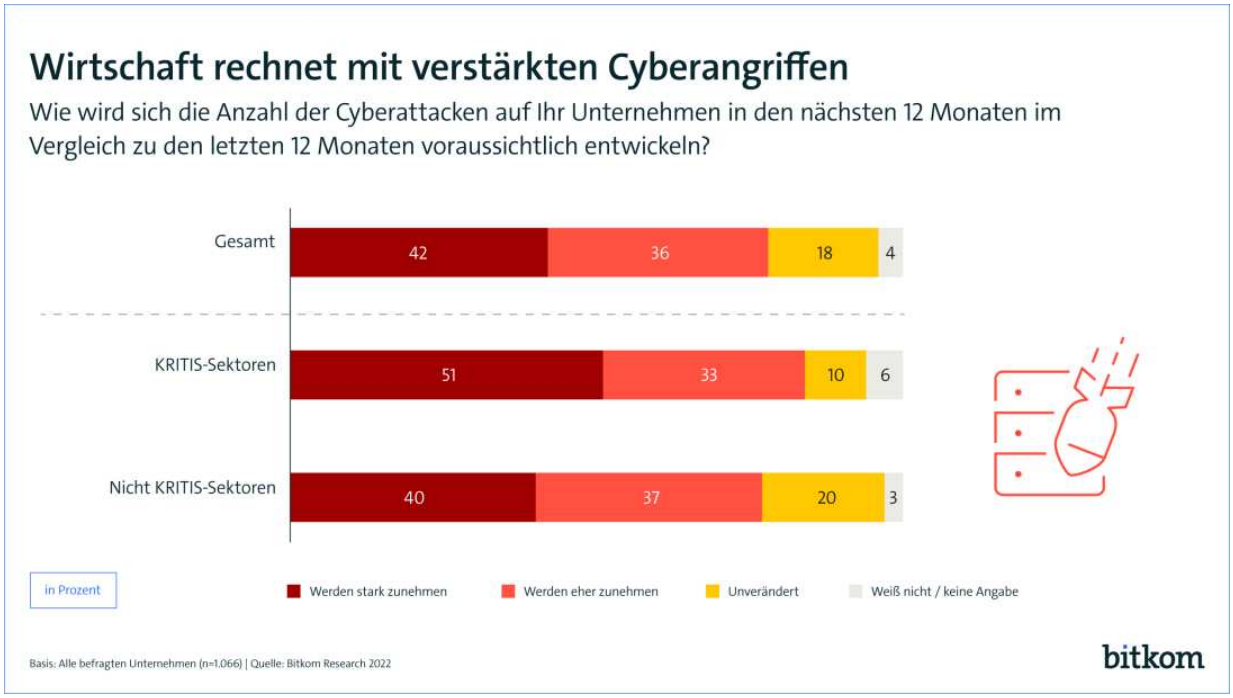
Der Großteil dieser Angriffe erfolgte gezielt – sowohl auf Betreiber Kritischer Infrastrukturen (KRITIS) als auch auf nicht KRITIS-Sektoren– durch organisierte Kriminalität oder durch Privatpersonen (Cracker), die vorsätzlich handeln.

- 15 Millionen Meldungen zu Schadprogramm-Infektionen in Deutschland übermittelte das BSI im Berichtszeitraum an deutsche Netzbetreiber.

- 34.000 Mail mit Schadprogrammen wurden monatlich durchschnittlich in deutschen Regierungsnetzen abfangen.

- 90% des Mail-Betrugs im Berichtszeitraum war Finance Phishing, d.h. die Mails erweckten betrügerisch den Eindruck, von Banken oder Sparkassen geschickt worden zu sein.

- 20.174 Schwachstellen in Software-Produkten (13% davon kritisch) wurden im Jahr 2021 bekannt. Das entspricht einem Zuwachs von 10% gegenüber dem Vorjahr.



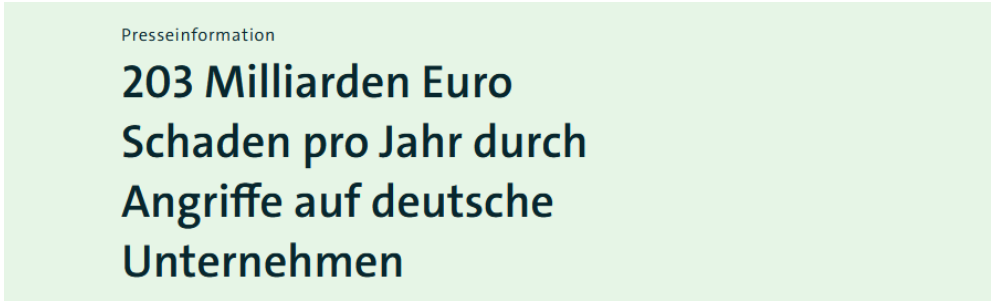
https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022#_

Diese Zahlen und Fakten zeigen, dass Cyberangriffe zu einem ernsthaften Risiko für Organisationen weltweit geworden sind. Forscher warnen zudem, dass der Reifegrad von KI-Technologien wie ChatGPT die Anzahl der Cyberangriffe ab dem Jahr 2023 erhöhen könnte. Daher gilt es proaktiv angemessene Maßnahmen zur Absicherung zu treffen – sowohl technisch als auch organisatorisch.

04. Die Kosten und Folgen von Cyberangriffen sind enorm

Kosten und Folgen eines Cyberangriffs

Die Folgen und Kosten eines Cyberangriffs können je nach Art und Umfang des Angriffs erheblich variieren. Laut einer Studie der Bitkom im Jahr 2022 waren mehr als 84% von 1.000 befragten Organisationen aus verschiedenen Branchen in Deutschland von Cyberangriffen betroffen. Darunter fielen hauptsächlich der Diebstahl sensibler Daten, das Ausspähen digitaler Kommunikationen und Sabotage von Systemen oder Betriebsabläufen. Der dabei entstandene Schaden in Deutschland beläuft sich der Studie zufolge auf über 203 Mrd. Euro.



https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022#_

Hier eine Aufstellung der häufigsten Kosten, die mit einem Cyberangriff verbunden sein können:

- Datenverlust oder Datenbeschädigung:
  Ein Cyberangriff kann dazu führen, dass wichtige Daten verloren gehen oder beschädigt werden, was für die Organisation möglicherweise schwerwiegende Folgen hat. Es kann auch dazu führen, dass sensible Daten in die Hände von Angreifern gelangen und für kriminelle Zwecke missbraucht werden.

- Geschäftsunterbrechung:
  Ein schwerwiegender Cyberangriff kann dazu führen, dass eine Organisation gezwungen ist, seinen Betrieb vorübergehend einzustellen, um das Problem zu beheben. Dies kann zu erheblichen finanziellen Verlusten führen, insbesondere wenn die Organisation nicht in der Lage ist, seine Kund*innen und Lieferant*innen zu bedienen.

- Reputationsverlust:
  Ein Cyberangriff kann das Vertrauen der Kund*innen in die Organisation erschüttern, was zu einem Verlust von Kund*innen und Einnahmen führen kann. Es kann auch den Ruf der Organisation und ggf. seine Marke beeinträchtigen.

- Wiederherstellung und Reparatur:
  Die Kosten für die Wiederherstellung von Systemen und Daten nach einem Cyberangriff können erheblich sein, insbesondere wenn es sich um einen schwerwiegenden Angriff handelt, der zu Datenverlust oder zur Beschädigung von Systemen führt.

- Haftungsrisiko:
  Wenn durch den Cyberangriff personenbezogene Daten von Kund*innen gestohlen wurden, kann die Organisation für die Verletzung von Datenschutzbestimmungen haftbar gemacht werden. Dies kann zu hohen Geldbußen und Strafen führen.

- Anwaltskosten:
  Organisationen können auch Anwaltskosten für die rechtliche Abwehr von Ansprüchen und Klagen im Zusammenhang mit dem Cyberangriff entstehen.

Insgesamt können die Folgen eines Cyberangriffs für Organisationen erheblich sein und langfristige Auswirkungen auf ihr Geschäft und ihren Ruf haben. Es ist daher wichtig, dass Organisationen eine robuste Cyber-Sicherheitsstrategie implementieren, um das Risiko von Cyberangriffen zu minimieren und, dass eine robuste Cyber-Sicherheitsstrategie implementiert wird, um im Falle eines Angriffs schnell und effektiv reagieren zu können.

Welche Maßnahmen sind nach einem Cyberangriff zu treffen?

Nach einem Cyberangriff muss eine Organisation eine Reihe von Maßnahmen ergreifen, um die Schäden zu begrenzen und das System wiederherzustellen. Wir zeigen dir hierzu im Folgenden einige effektive Schritte, die Organisationen nach einem Cyberangriff unternehmen sollten:

- Isolierung der betroffenen Systeme:
  Die Organisation sollte die betroffenen Systeme isolieren, um die Ausbreitung des Angriffs auf andere Systeme zu verhindern.

- Bewertung des Schadens:
  Die Organisation sollte den Umfang des Angriffs bewerten und feststellen, welche Systeme, Daten oder Anwendungen betroffen sind.

- Sammlung von Beweisen:
  Die Organisation sollte Beweise über den Angriff sammeln, um den / die Angreifer*in zu identifizieren und ggf. verfolgen zu können.

- Information der Betroffenen:
  Die Organisation sollte die betroffenen Mitarbeiter*innen, Kund*innen und andere Stakeholder über den Angriff informieren und ihnen Anweisungen bzw. Informationen zum weiteren Vorgehen geben.

- Wiederherstellung der Daten und Systeme:
  Die Organisation sollte seine Daten und Systeme aus Backups wiederherstellen oder gegebenenfalls neu aufbauen.

- Überprüfung der Sicherheitslücken:
  Die Organisation sollte die Sicherheitslücken identifizieren, die zu dem Angriff geführt haben, und geeignete Maßnahmen ergreifen, um zukünftige Angriffe zu verhindern.

- Überwachung der Systeme:
  Die Organisation sollte seine Systeme sorgfältig überwachen, um sicherzustellen, dass keine weiteren Angriffe stattfinden.

- Schulung der Mitarbeiter:
  Die Organisation sollte seine Mitarbeiter regelmäßig über die Bedeutung von Cyber-Sicherheit und die besten Praktiken im Umgang mit sensiblen Daten schulen.

Es ist wichtig zu beachten, dass die Wiederherstellung eines Systems nach einem Cyberangriff ein komplexer Prozess ist, der Zeit und Ressourcen erfordert. Eine schnelle Reaktion auf den Angriff durch die Mitarbeiter*innen der Organisation und eine umfassende Vorbereitung sind unerlässlich, um die Auswirkungen des Angriffs zu minimieren und die Organisation schneller wieder auf den richtigen Weg zu bringen.

An welche Stellen kann ich mich nach einem Cyberangriff wenden?

Wenn deine Organisation Opfer eines Cyberangriffs geworden ist, gibt es mehrere Stellen, an die du dich wenden kannst.

- BSI:
  Du kannst das Bundesamt für Sicherheit in der Informationstechnik (BSI) kontaktieren, um Unterstützung bei der Abwehr des Angriffs zu erhalten. Das BSI bietet auch allgemeine Beratung und Schulungen zur IT-Sicherheit an.

- CERT:
  Du kannst dich auch an ein Computer Emergency Response Team (CERT) wenden. Es gibt verschiedene CERT-Teams, die dir je nach Art des Angriffs und deiner Situation helfen können. Du kannst beispielsweise das CERT-Bund des BSI oder ein privates CERT-Team kontaktieren.

- Polizei:
  Du kannst auch die Polizei einschalten, insbesondere wenn es sich um einen schwerwiegenden Angriff oder eine Straftat handelt. Die Polizei kann Ermittlungen aufnehmen und dir bei der Bewältigung des Angriffs helfen.

- IT-Sicherheitsunternehmen:
  Es gibt viele Organisationen, die sich auf IT-Sicherheit spezialisiert haben und dir bei der Bewältigung des Angriffs helfen kann. Du kannst beispielsweise IT-Sicherheitsdienstleister*innen oder Forensik-Expert*innen kontaktieren.

- Anwalt:
  Wenn der Angriff rechtliche Konsequenzen hat, kannst Du auch einen Anwalt / eine Anwältin einschalten, der/die dir bei rechtlichen Fragen und Schadensersatzforderungen helfen kann.

In jedem Fall ist es wichtig, schnell zu handeln und professionelle Hilfe in Anspruch zu nehmen, um den Schaden zu begrenzen und zukünftige Angriffe zu verhindern.

05. Rechtliche Pflichten der Organisation nach einem Cyberangriff

Wenn eine Organisation Opfer eines Cyberangriffs wird, hat diese bestimmte rechtliche Pflichten, insbesondere im Hinblick auf den Schutz der betroffenen Daten und die Informationspflicht gegenüber den Betroffenen.

- Meldepflicht:
  Organisationen sind in der Regel gesetzlich verpflichtet, bestimmte Arten von Datenschutzverletzungen an die zuständige Aufsichtsbehörde zu melden. In Deutschland ist dies in der Regel die Landesdatenschutzbehörde. Die Meldepflicht besteht insbesondere bei Verletzungen des Schutzes personenbezogener Daten.

- Informationspflicht:
  Organisationen müssen auch die betroffenen Personen über den Vorfall informieren, insbesondere wenn es sich um eine Datenschutzverletzung handelt. Die Information muss in der Regel schnellstmöglich und in verständlicher Sprache erfolgen.

- Schutzmaßnahmen:
  Organisationen sind verpflichtet, angemessene technische und organisatorische Maßnahmen (TOM) zu ergreifen, um die betroffenen Daten zu schützen und zukünftige Angriffe zu verhindern. Wenn diese Pflicht verletzt wird, kann dies rechtliche Konsequenzen haben.

- Schadensersatz:
  Wenn der Angriff zu einem Schaden führt, können die Betroffenen Schadensersatzansprüche gegen die Organisation geltend machen. Die Organisation ist verpflichtet, den Schaden zu ersetzen, wenn es den Angriff verursacht hat oder seine Schutzpflichten verletzt hat.

KRITIS - Beachtung besonderer Pflichten

Für Kritische Infrastrukturen (KRITIS) gibt es nach einem Cyberangriff gesonderte Pflichten. KRITIS sind Organisationen, die für die Aufrechterhaltung wichtiger Infrastrukturen und Dienstleistungen verantwortlich sind, wie z.B. Energieversorgung, Wasser- und Abwasserversorgung, Gesundheitswesen oder Telekommunikation. Diese Organisationen haben eine besondere Verantwortung, um sicherzustellen, dass ihre Dienste auch in Zeiten von Krisen und Angriffen verfügbar sind.

Zu den besonderen Pflichten von Betreibern Kritischer Infrastrukturen nach einem Cyberangriff gehören gemäß IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0):

- Meldung an das BSI: Betreiber Kritischer Infrastrukturen sind verpflichtet, bestimmte Arten von Cyberangriffen und IT-Sicherheitsvorfällen unverzüglich dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden. Das BSI kann dann bei der Analyse und Bewältigung des Vorfalls unterstützen.

- Notfallpläne: Betreiber Kritischer Infrastrukturen müssen über angemessene Notfallpläne verfügen, um sicherzustellen, dass ihre Dienste auch im Falle eines Cyberangriffs aufrechterhalten werden können. Diese Pläne sollten regelmäßig getestet und aktualisiert werden, um sicherzustellen, dass sie im Ernstfall effektiv sind.

- Zusammenarbeit mit Behörden: Betreiber Kritischer Infrastrukturen sind verpflichtet, eng mit den zuständigen Behörden zusammenzuarbeiten, um den Vorfall zu bewältigen und die Auswirkungen auf die Bevölkerung und die Infrastruktur zu minimieren.

- Schutz von sensiblen Daten: Betreiber Kritischer Infrastrukturen müssen sicherstellen, dass sensible Daten, wie z.B. personenbezogene Daten oder Geschäftsgeheimnisse, angemessen geschützt sind und nicht in die falschen Hände geraten.

- Regelmäßige Schulungen und Awareness-Programme: Betreiber Kritischer Infrastrukturen sollten ihre Mitarbeiter*innen regelmäßig schulen und sensibilisieren, um das Bewusstsein für IT-Sicherheit und Cyberangriffe zu schärfen.

Insgesamt müssen Betreiber Kritischer Infrastrukturen besonders proaktiv und vorausschauend agieren, um ihre Dienste und Informationen vor Cyberangriffen schützen, die Auswirkungen von Angriffen minimieren und somit ihre Pflichten erfüllen zu können.

Nach aktuellen Vorfällen und der politischen Lage in 2022 arbeitet das Innenministerium an einem KRITIS-Dachgesetz, das Anforderungen zu Resilienz und physischer Sicherheit an Kritische Infrastrukturen konkretisieren soll. Die

im jetzigen IT-Sicherheitsgesetz noch fehlenden Sektoren (und Branchen) könnten dann im IT-Sicherheitsgesetz 3.0 geregelt werden und zwar:

Teilweise in KRITIS:
Digitale Infrastruktur, Raumfahrt, Post und Kurier, Chemikalien, Industrie (Manufacturing), Digitale Dienste

Fehlt in KRITIS:
Energie (Wasserstoff), Gesundheit (Medizinforschung, Medizingeräte), ICT Service Management (Managed Security, Services Providers), öffentliche Verwaltung, Forschung (Forschungsinstitute)

06. Maßnahmen für höhere Cybersicherheit: So gehen Organisationen am besten vor

In den vorherigen Kapiteln haben wir die aktuelle Bedrohungslage, die Folgen und die damit verbundenen Kosten/Schäden eines Cyber-Angriffs näher beleuchtet.

Damit es aber erst gar nicht zu einem Cyber-Angriff kommt bzw. man das Risiko minimiert, können Organisationen viele proaktive Maßnahmen ergreifen, um die Cybersicherheit zu erhöhen. Hier sind einige wichtige Schritte, die zu berücksichtigen sind:

- Risikoanalyse:
  Organisationen sollten eine umfassende Risikoanalyse durchführen, um ihre Schwachstellen und Bedrohungen zu identifizieren. Hierbei sollten die Assets, die zu schützen sind, sowie die Art der Bedrohungen und die potenziellen Auswirkungen von Sicherheitsverletzungen berücksichtigt werden.

- Sicherheitsrichtlinien und -verfahren:
  Organisationen sollten klare Sicherheitsrichtlinien und -verfahren entwickeln und durchsetzen, um sicherzustellen, dass Mitarbeiter*innen, Partner*innen und Dritte die erforderlichen Sicherheitsmaßnahmen umsetzen.

- Mehrschichtige technische Sicherheitsmaßnahmen:
  Organisationen sollten eine Vielzahl von Sicherheitsmaßnahmen wie Firewalls, Intrusion Detection und Prevention, Antivirus-Software und Verschlüsselung einsetzen, um ihre Systeme und Daten zu schützen.

- Schulungen und Bewusstseinsbildung:
  Technische Schutzmaßnahmen alleine reichen heutzutage nicht mehr aus. Mitarbeiter*innen sollten daher regelmäßig geschult und auf die Bedeutung von Cybersicherheit und auf Best Practices sensibilisiert werden.

- Schwachstellenmanagement:
  Organisationen sollten regelmäßig Schwachstellen in ihren Systemen identifizieren und beheben, um Angriffspunkte für potenzielle Angreifer*innen zu minimieren.

- Incident Response Plan:
  Organisationen sollten einen ausgereiften Incident Response Plan entwickeln, um auf Sicherheitsverletzungen schnell und effektiv zu reagieren und die Auswirkungen minimieren zu können.

- Compliance:
  Organisationen sollten sicherstellen, dass sie die geltenden Vorschriften und Bestimmungen einhalten, um ihre Systeme und Daten zu schützen und Geldbußen und Reputationsverluste zu vermeiden.

Diese Schritte können dabei helfen, die Cybersicherheit zu erhöhen. Allerdings sollten Organisationen auch sicherstellen, dass sie auf dem neuesten Stand bleiben und sich kontinuierlich über die neuesten Bedrohungen und Sicherheitsmaßnahmen informieren, um ihre Systeme und Daten angemessen zu schützen.

On Premise- oder Cloudlösungen – Was ist sicherer?

Die Sicherheit von On-Premise-Lösungen (kurz: die Software wird auf eigener / angemieteter Hardware installiert) und Cloud-Lösungen (kurz: die Software wird im Rechenzentrum des/ der Lizenzgeber*in gehostet) hängt von verschiedenen Faktoren ab und kann nicht pauschal beantwortet werden. Beide Ansätze haben ihre Vor- und Nachteile in Bezug auf Sicherheit.

On-Premise-Lösungen können eine höhere Kontrolle und Anpassbarkeit bieten, da Organisationen direkt für die Sicherheit ihrer Systeme und Daten verantwortlich sind. Allerdings kann dies auch bedeuten, dass Organisationen mehr Zeit und Ressourcen investieren müssen, um ihre Systeme und Daten angemessen zu schützen. On-Premise-Lösungen können auch anfälliger für physische Angriffe und interne Bedrohungen sein.

Cloud-Lösungen hingegen bieten oft eine höhere Skalierbarkeit und Automatisierung von Sicherheitsmaßnahmen wie DDoS-Schutz und Netzwerksegmentierung. Cloud-Provider verfügen oft über umfangreiche Erfahrung und Ressourcen, um die Sicherheit ihrer Systeme und Daten zu gewährleisten. Allerdings kann die Abhängigkeit von Cloud-Providern auch ein Sicherheitsrisiko darstellen, insbesondere wenn Organisationen keine umfassende Due Diligence (kurz: Überprüfung des/ der Geschäftspartner*in bei der Aufnahme einer neuen Geschäftsbeziehung) durchgeführt haben und sich ohne Prüfung auf den Cloud-Provider verlassen, um ihre Sicherheit zu gewährleisten.

Insgesamt hängt die Sicherheit von On-Premise- und Cloud-Lösungen von der Umsetzung und Implementierung der Sicherheitsmaßnahmen ab. Beide Ansätze können sicher sein, solange die Sicherheitsmaßnahmen auf dem neuesten Stand gehalten und angemessen implementiert werden. Organisationen müssen ihre Sicherheitsanforderungen und die Bedrohungslandschaft berücksichtigen und eine fundierte Entscheidung treffen, welcher Ansatz am besten zu ihren Bedürfnissen passt.

Vor- und Nachteile von On-Premise- und Cloudlösungen im Bereich der Cybersicherheit

On-Premise und Cloud sind zwei gängige Ansätze zur Implementierung von Cyber-Sicherheitslösungen, und beide haben Vor- und Nachteile, die wir dir nachfolgend einmal übersichtlich aufgelistet haben.

On-Premise-Lösung:

PRO

Direkte Kontrolle: Organisationen haben direkte Kontrolle über ihre Systeme und Daten und können ihre Sicherheitsmaßnahmen selbst steuern.

Anpassbarkeit: Organisationen können ihre Sicherheitslösungen an ihre spezifischen Anforderungen anpassen und zusätzliche Sicherheitsfunktionen hinzufügen.

Datenhoheit: Organisationen können sicherstellen, dass ihre Daten innerhalb der Unternehmensgrenzen verbleiben und nicht an Dritte weitergegeben werden.

Hohe Kosten: Die Implementierung und der Betrieb von On-Premise-Lösungen erfordern in der Regel hohe Investitionen in Infrastruktur, Personal und Wartung.

Skalierbarkeit: On-Premise-Lösungen könne schwer skalierbar sein und erfordern möglicherweise zusätzliche Investitionen, um die Kapazität zu erhöhen.

Veraltete Technologie: Organisationen müssen ihre Technologie ständig aktualisieren und auf dem neuesten Stand halten, um mit der sich schnell verändernden Bedrohungslandschaft Schritt zu halten.

CONTRA

Cloud-Lösung:

PRO

Kosteneffektivität: Cloud-Lösungen sind in der Regel kosteneffektiver als On-Premise-Lösungen, da Organisationen nur für die Nutzung bezahlen, ohne sich um die Wartung und den Betrieb kümmern zu müssen.

Skalierbarkeit: Cloud-Lösungen sind hochgradig skalierbar und können schnell an sich ändernde Anforderungen angepasst werden.

Automatisierte Sicherheitsmaßnahmen: Cloud-Provider bieten oft automatisierte Sicherheitsmaßnahmen wie DDoS-Schutz, Netzwerksegmentierung und Verschlüsselung an.

Abhängigkeit vom Provider: Organisationen sind von ihrem Cloud-Provider abhängig, um die Verfügbarkeit ihrer Systeme und die Vertraulichkeit sowie Integrität ihrer Daten zu schützen.

Datensicherheit: Organisationen müssen sicherstellen, dass ihre Daten in der Cloud sicher sind und dass der Cloud-Provider robuste Sicherheitsmaßnahmen implementiert hat.

Compliance: Einige Branchen haben strenge Compliance-Anforderungen, die es schwierig machen können, Cloud-Lösungen zu nutzen.

CONTRA

Zentral für eine passende Lösung sind die individuellen Anforderungen der jeweiligen Organisation, aus diesem Grund kann nur unter Berücksichtigung aller für sie relevanten Aspekte eine fundierte Entscheidung getroffen werden.

MORGENSTERN
als externer Informationssicherheitsbeauftragter

- Unterstützung der Schutzziele nach Brachenstandards
- Zentrale Anlaufstelle
- Überprüfung von Sicherheitszielen, -richtlinien und -dokumenten
- Vorbereitung und Begleitung von Penetrationstests
- Beratung der Geschäftsleitung in strategischen Fragen der Informationssicherheit

Unsere Inhouse-Angebote gibt es für jedes Unternehmen. Wir organisieren individuelle, auf dich und dein Unternehmen zugeschnittene Inhouse-Schulungen zu Themen wie

- Digitale*r Schatzhüter*in – Informationssicherheit im Finanzsektor
- Informationssicherheit in der Automobilbranche (TISAX)
- Informationssicherheitsbeauftragte*r (IHK)
- Microsoft 365 | Wolkig mit Aussicht auf Datenschutz
- PCI | Verstehen und Umsetzen des Sicherheitsstandards für Kreditkarten
- Software- und Lizenzmanagement | Wege zur digitalen Compliance und Effizienz
- Systemmonitoring und Load Balancing

the future is yours.

IT-Sicherheitsbeauftragte von MORGENSTERN wissen, welche Vorgaben eingehalten werden müssen, kennen die Herausforderungen, die das Thema mit sich bringt und leiten und koordinieren die Projekte von extern, falls deine Mitarbeiter*innen dabei Unterstützung brauchen. Auch für die Einhaltung der internationalen Sicherheitsstandards sorgen wir und geben dir die notwendigen Handlungsempfehlungen.

Basis

bis zu **3h** im Monat inklusive

+

Zusatzleistungen

Preis auf Anfrage

Premium

bis zu **8h** im Monat inklusive

+

Zusatzleistungen

Preis auf Anfrage

Pro

bis zu **16h** im Monat inklusive

+

Zusatzleistungen

Preis auf Anfrage

zentrale Angebotsleistungen

- Zentrale Ansprechpartner*in für alle Fragen der Informationssicherheit
- Beratung der Geschäftsleitung in strategischen Fragen der Informationssicherheit
- Beratung im Zusammenhang mit Risikoanalysen
- Compliance-Unterstützung / Audit-Vorbereitung
- Reaktionszeitraum innerhalb von 5 Werktagen

zentrale Zusatzleistungen

- Vergünstigter Zugang zur MORGENSTERN E-Learning Plattform und Inhalten der Informationssicherheit
- Vergünstigte Durchführung von Phishing-Kampagnen (nur im Pro-Package enthalten)

07. Glossar: Hacker, Malware, Ransomware & Co - was steckt hinter diesen Be griffen?

Hacker sind Personen, die sich daran freuen, ein tiefgehendes Verständnis um die Arbeitsweise eines Systems, insbesondere von Rechnern und Rechnernetzen, zu erlangen. Sie halten sich an die Hackerethik und führen keine illegalen Aktionen durch.

Es gibt verschiedene Arten von Hackern:

- White-Hat-Hacker: auch bekannt als "Ethical Hacker", arbeiten für Organisationen, um Schwachstellen in deren Systemen zu finden und diese zu beheben.
- Black-Hat-Hacker: auch bekannt als "Kriminelle Hacker", nutzen ihre Fähigkeiten, um illegal in Systeme einzudringen, um Daten zu stehlen, Schaden zu verursachen oder Geld zu erpressen.
- Grey-Hat-Hacker: diese Art von Hackern haben keine böswilligen Absichten, aber sie handeln nicht im Auftrag einer Organisation und können ohne Erlaubnis auf Systeme zugreifen.
- Script-Kiddies: Personen ohne tiefgreifende Kenntnisse, die vorgefertigte Tools und Skripte verwenden, um Systeme anzugreifen.

Es ist wichtig zu beachten, dass – entgegen der häufigen medialen Darstellung – nicht alle Hacker Kriminelle sind und aus bösartigen Absichten handeln. Vielmehr nutzen viele von ihnen ihr Wissen und ihre Fähigkeiten, um Systeme sicherer zu machen oder um in der IT-Branche zu arbeiten. Es ist jedoch auch wichtig zu verstehen, dass illegale Aktivitäten wie das Eindringen in fremde Systeme ohne Zustimmung oder das Stehlen von Daten illegal sind und schwerwiegende strafrechtliche Konsequenzen haben können.

Cracker Ein Cracker ist eine Person, die sich in Computersysteme oder Netzwerke einloggt, um Schaden zu verursachen, zu stehlen oder zu manipulieren. Im Gegensatz zu einem Hacker hat ein Cracker keine moralischen Grenzen und handelt aus böswilligen Motiven, um seine eigenen Interessen zu verfolgen.

Ein Cracker kann verschiedene Arten von Angriffen durchführen, einschließlich des Eindringens in Systeme, um vertrauliche Informationen zu stehlen, die Zerstörung oder Manipulation von Daten oder die Übernahme der Kontrolle über ein System oder Netzwerk, um diese für eigene Zwecke zu nutzen.

Cracker nutzen oft Schwachstellen in Systemen oder Netzwerken aus, um Zugriff zu erlangen und ihre kriminellen Aktivitäten auszuführen. Sie können auch Social-Engineering-Techniken (s.h. Seite 17) nutzen, um Benutzer*innen zu täuschen und Zugang zu sensiblen Informationen zu erhalten.

Hacktivist Ein Hacktivist ist eine Person oder Gruppe von Personen, die ihre Fähigkeiten im Bereich der Computersicherheit nutzen, um politische oder soziale Botschaften zu verbreiten oder um politische oder soziale Veränderungen zu bewirken. Im Gegensatz zu Crackern oder Black-Hat-Hackern handeln Hacktivisten in der Regel aus ideologischen Gründen und wollen auf bestimmte politische oder soziale Themen aufmerksam machen oder Veränderungen in der Gesellschaft herbeiführen.

Hacktivisten können verschiedene Arten von Angriffen durchführen, um ihre Botschaft zu verbreiten oder Informationen öffentlich zu machen, einschließlich Distributed-Denial-of-Service (DDoS)-Angriffe, defacing von Websites, Social-Engineering-Attacken und Offenlegen von Informationen. Berühmte Hacktivistengruppen sind z.B. Anonymous oder LulzSec, die in der Vergangenheit für Angriffe auf Regierungs- und Unternehmensnetzwerke verantwortlich waren.

Es ist wichtig zu beachten, dass die meisten Hacktivisten ihre Aktivitäten als politischen Aktivismus sehen und nicht als kriminelle Handlungen. Allerdings können Hacktivisten durch ihr Tun unbeabsichtigt in die Kriminalität rutschen und dadurch rechtliche Konsequenzen riskieren.

Malware ist ein Sammelbegriff für schädliche Software, die dazu entwickelt wurde, Computer, Netzwerke oder Mobilgeräte ohne Zustimmung des/ der Besitzers/

Besitzerin zu infiltrieren oder zu beschädigen. Die Bezeichnung "Malware" ist eine Abkürzung für "Malicious Software" (bösartige Software).

Es gibt verschiedene Arten von Malware, darunter Viren, Trojaner, Würmer, Ransomware, Adware und Spyware.

Virus Ein Virus ist eine Art von schädlicher Software, die sich selbst replizieren und in andere Computerprogramme oder Systeme einschleusen kann, um sich zu verbreiten und Schaden zu verursachen. Ein Virus kann sich auf einem Computer installieren, indem er eine Schwachstelle im System ausnutzt oder sich als legitimes Programm tarnt, das der Benutzer freiwillig herunterlädt und ausführt.

Einmal im System installiert, kann ein Virus verschiedene schädliche Aktivitäten ausführen, wie z.B. das Löschen oder Ändern von Daten, das Unterbrechen der Systemfunktionalität oder das Ausspähen vertraulicher Informationen. Einige Viren können sich auch selbst in E-Mails oder Dateianhängen verbreiten und so andere Computer infizieren.

- Computerviren können in verschiedene Kategorien eingeteilt werden, je nach ihrer Funktionsweise oder der Art des Schadens, den sie verursachen.

  Einige der bekanntesten Virentypen sind:

  - Dateivirus: Dieser Virentyp infiziert Dateien, indem er seinen Code in sie einbettet und sich bei jeder Ausführung des infizierten Programms aktiviert.

  - Bootsektorvirus: Diese Art von Virus infiziert den Bootsektor der Festplatte und kann den Computer unbrauchbar machen, indem er die Startfunktionen des Betriebssystems stört.

  - Makrovirus: Diese Art von Virus infiziert Dokumente und Dateien, die Makros enthalten, wie z.B. Word-Dokumente oder Excel-Tabellen. Wenn ein infiziertes Dokument geöffnet wird, aktiviert sich der Virus und kann schädliche Aktionen ausführen.

  - Rootkit: Ein Rootkit ist eine Art von Virus, der sich tief im System versteckt und es dem Angreifer ermöglicht, unbemerkt auf das System zuzugreifen und es zu steuern.

Trojaner Ein Trojaner (auch Trojanisches Pferd genannt) ist eine Art von schädlicher Software, die sich als legitime Anwendung tarnt, um unbemerkt in ein Computersystem einzudringen und Schaden zu verursachen. Der Name stammt aus der griechischen Mythologie, in der das Trojanische Pferd als List verwendet wurde, um Troja zu infiltrieren.

Ein Trojaner verbreitet sich normalerweise nicht von selbst, sondern wird vom Benutzer absichtlich oder unwissentlich heruntergeladen und installiert. Einmal im System aktiviert, kann der Trojaner verschiedene schädliche Aktionen ausführen, wie z.B. das Löschen von Dateien, das Ausspähen von vertraulichen Informationen, das Öffnen einer Hintertür für einen Angreifer oder die Installation von weiterer Malware auf dem infizierten System.
Es gibt verschiedene Arten von Trojanern, die für unterschiedliche Zwecke entwickelt wurden. Einige der bekanntesten Arten sind:

- Backdoor-Trojaner: Diese Art von Trojaner öffnet eine Hintertür auf dem infizierten System, um einem Angreifer den Zugriff auf das System zu ermöglichen.

- Keylogger-Trojaner: Diese Art von Trojaner zeichnet alle Tastatureingaben des Benutzers auf und kann so vertrauliche Informationen wie Passwörter und Kontodaten stehlen.

- Banking-Trojaner: Diese Art von Trojaner zielt darauf ab, Bankdaten und andere vertrauliche Informationen von Benutzern zu stehlen, indem er sich in Online-Banking- oder Zahlungs-Apps einschleust.

- Ransomware-Trojaner: Diese Art von Trojaner sperrt den Zugriff auf bestimmte Dateien oder das gesamte System und fordert vom Benutzer eine Lösegeldzahlung, um den Zugriff wiederherzustellen

Wurm Ein Computerwurm ist eine Art von Schadsoftware, die sich selbstständig innerhalb eines Computersystems oder Netzwerks verbreitet, indem sie Schwachstellen ausnutzt oder sich über Netzwerkdienste und -protokolle ausbreitet. Im Gegensatz zu einem Computervirus benötigt ein Wurm keine ausführbare Datei, um sich zu verbreiten, sondern nutzt vorhandene Systemressourcen und Netzwerkdienste.

Ein Computerwurm kann verschiedene Arten von Schaden anrichten, je nach seinen spezifischen Funktionen und Zwecken.

Einige der häufigsten Schadensarten sind:

- Verbreitung anderer Malware: Ein Wurm kann so programmiert sein, dass er andere Malware auf dem infizierten System installiert oder herunterlädt.
- Netzwerküberlastung: Ein Wurm kann das Netzwerk durch die Übertragung großer Datenmengen überlasten und so die Netzwerkleistung beeinträchtigen oder sogar zum Absturz bringen.
- Datendiebstahl: Ein Wurm kann vertrauliche Informationen wie Passwörter, Kontoinformationen oder andere persönliche Daten sammeln und an einen Remote-Server senden.
- Zerstörung von Daten: Ein Wurm kann Dateien löschen oder das gesamte System unbrauchbar machen.

Einige der bekanntesten Würmer in der Geschichte der Computersicherheit sind der Morris-Wurm, der im Jahr 1988 das Internet infizierte, der ILOVEYOU-Wurm, der im Jahr 2000 eine der größten E-Mail-basierten Malware-Attacken verursachte, und der WannaCry-Wurm, der im Jahr 2017 eine globale Ransomware-Epidemie auslöste.

Rootkit Ein Rootkit ist eine Art von Malware, die darauf abzielt, eine tiefgreifende und langfristige Kontrolle über ein infiziertes Computersystem zu erlangen. Im Allgemeinen zielt ein Rootkit darauf ab, seinen eigenen Zugriff auf das Betriebssystem und dessen Funktionen zu verschleiern, um nicht entdeckt zu werden.
Ein Rootkit kann auf verschiedene Arten implementiert werden. Einige werden als eigenständige Programme installiert, während andere in andere Malware integriert werden, wie z.B. Trojaner, Viren oder Würmer. Ein Rootkit kann auch als Teil eines Exploits genutzt werden, um eine Schwachstelle im System auszunutzen und Administrator- oder Root-Rechte zu erlangen.

Einige der Hauptfunktionen eines Rootkits können sein:

- Verschleierung: Ein Rootkit kann seine eigene Existenz oder Aktivität vor dem Benutzer und Antivirus-Programmen verbergen, indem es den Zugriff auf wichtige Systemdateien blockiert oder seinen eigenen Prozess verbirgt.
- Überwachung und Datenerfassung: Ein Rootkit kann in der Lage sein, den Netzwerkverkehr zu überwachen, Benutzereingaben zu protokollieren, Tastatureingaben aufzuzeichnen oder Bildschirmaufnahmen zu machen, um vertrauliche Informationen zu stehlen.
- Fernsteuerung: Ein Rootkit kann ein Backdoor in das System öffnen, um einem Angreifer den Fernzugriff und die Kontrolle über das System zu ermöglichen.
- Modifikation: Ein Rootkit kann Dateien oder Konfigurationen im System ändern, um seine eigenen Ziele zu erreichen, wie z.B. das Herunterladen von zusätzlicher Malware oder das Blockieren von Sicherheits-Updates.

Spyware ist eine Art von Schadsoftware, die heimlich auf einem Computer, Mobilgerät oder einem anderen Gerät installiert wird, um Informationen zu sammeln und an einen Dritten zu übermitteln, ohne dass der Benutzer es bemerkt.

Die Spyware kann auf verschiedene Weise auf das Gerät gelangen, z.B. über das Herunterladen von infizierten Dateien, die Installation von bösartigen Apps oder durch das Ausnutzen von Sicherheitslücken im Betriebssystem oder in Anwendungen.

Einmal installiert, kann Spyware verschiedene Aktionen ausführen, wie z.B. das Protokollieren von Tastatureingaben, das Überwachen von Webseitenbesuchen und sonstige Aktivitäten, das Sammeln von Passwörtern und

anderen vertraulichen Informationen oder das Aufzeichnen von Audio- und Videoaufnahmen.

Die gesammelten Daten können dann an einen entfernten Server oder einen Hacker weitergeleitet werden, der sie für kriminelle Zwecke nutzen kann. Die Nutzung von Spyware kann dazu führen, dass die Privatsphäre von Einzelpersonen und Unternehmen verletzt wird, da sie es Kriminellen ermöglicht, sensible Daten zu stehlen oder zu missbrauchen.

Ransomware ist eine Art von Malware, die darauf abzielt, den Zugriff auf ein Computersystem, ein Netzwerk oder bestimmte Dateien zu sperren oder zu verschlüsseln und dann ein Lösegeld zu erpressen, um den Zugriff wiederherzustellen. Ransomware wird in der Regel über Phishing-E-Mails, infizierte Websites oder Social-Engineering-Methoden verbreitet.

Sobald die Ransomware auf dem Opfersystem ausgeführt wird, verschlüsselt sie die Dateien und fordert dann ein Lösegeld in der Regel in Form von Kryptowährungen, um den Zugriff auf die Dateien wiederherzustellen. Die Höhe des Lösegelds variiert je nach Art der Ransomware und den Anforderungen des Angreifers.

Es ist wichtig zu beachten, dass es keine Garantie gibt, dass das Lösegeld, tatsächlich dazu führt, dass die verschlüsselten Dateien wiederhergestellt werden. In einigen Fällen haben die Opfer trotz Zahlung des geforderten Betrags keinen Zugriff auf ihre Dateien erhalten oder wurden erneut von den Angreifern erpresst.

Ransomware as a Service (RaaS) ist ein Geschäftsmodell, bei dem Kriminelle Ransomware als Service anbieten, indem sie anderen Kriminellen eine Ransomware-Plattform zur Verfügung stellen, die sie nutzen können, um Opfer anzugreifen und zu erpressen. Diese Plattformen sind oft benutzerfreundlich gestaltet und erfordern nur minimale technische Fähigkeiten, um sie zu nutzen.

Mit RaaS können Cyberkriminelle schnell und einfach Ransomware-Angriffe durchführen, ohne die notwendigen Fähigkeiten oder Ressourcen zu haben, um ihre eigene Ransomware zu entwickeln. Die Anbieter von RaaS erhalten in der Regel eine Provision von den Kriminellen, die ihre Plattform nutzen, wobei die Höhe der Provision von den erzielten Einnahmen abhängt.

Social Engineering ist eine Form von Angriffen auf Computersysteme und Netzwerke, bei denen anstelle von technischen Schwachstellen menschliche Schwachstellen ausgenutzt werden. Dabei nutzen Angreifer Täuschung, Manipulation und Überredungskunst, um Menschen dazu zu bringen, vertrauliche Informationen preiszugeben oder unautorisierten Zugang zu einem Computersystem oder Netzwerk zu gewähren.

Ein Beispiel für Social Engineering könnte eine E-Mail oder ein Anruf sein, der vorgibt, von einem vertrauenswürdigen Absender wie einem / einer Bankmitarbeiter*in, einem / einer IT-Administrator*in oder einem / einer Kundenbetreuer*in zu stammen. In der E-Mail oder im Anruf wird dann möglicherweise der /die Empfänger*in aufgefordert, vertrauliche Informationen preiszugeben, wie z.B. Benutzernamen, Passwörter oder Kreditkarteninformationen. Wenn der/ die Empfänger*in auf diese Anfragen eingeht, kann dies zu einem Datenverlust oder zu unautorisiertem Zugriff auf das Netzwerk führen.

Phishing ist eine Form von Cyberangriff, bei der Angreifer gefälschte E-Mails, Nachrichten oder Websites erstellen, um vertrauliche Informationen wie Benutzernamen, Passwörter, Kreditkartennummern und andere persönliche Daten von Opfern zu stehlen. Phishing-Angriffe zielen darauf ab, Opfer zu täuschen, um sie dazu zu bringen, ihre vertraulichen Informationen preiszugeben oder Malware auf ihren Systemen zu installieren.

Phishing-Angriffe können in verschiedenen Formen auftreten, wie z.B.:

- Spear Phishing: Zielgerichtete Phishing-Angriffe, bei denen Angreifer speziell auf bestimmte Personen oder Unternehmen abzielen, um vertrauliche Informationen zu stehlen oder Malware zu installieren.
- Clone Phishing: Angriffe, bei denen Angreifer E-Mails mit gefälschtem Absender und gefälschtem Inhalt senden, die aussehen, als kämen sie von einer vertrauenswürdigen Quelle oder einer zuvor gesendeten legitimen E-Mail.
- Pharming: Eine Art von Angriff, bei der Angreifer die DNS-Einträge einer legitimen Website manipulieren, um Opfer auf gefälschte Websites umzuleiten.

Spear-Phishing ist eine spezielle Form des Phishing-Angriffs, bei dem die Angreifer gezielt bestimmte Personen oder Organisationen ins Visier nehmen, um vertrauliche Informationen zu stehlen oder finanzielle Schäden zu verursachen.

Im Gegensatz zu traditionellen Phishing-Angriffen, bei denen in der Regel eine große Anzahl von E-Mails an zufällige Empfänger gesendet wird, ist Spear Phishing gezielter und personalisierter. Die Angreifer recherchieren in der Regel im Vorfeld über ihre Ziele, um deren Interessen und Arbeitsumfeld besser zu verstehen und zu nutzen.

Die Spear-Phishing-E-Mails sind oft sehr gut formuliert und enthalten häufig personalisierte Informationen, die dazu beitragen, das Vertrauen der Opfer zu gewinnen und sie dazu zu veranlassen, auf einen bösartigen Link zu klicken oder eine infizierte Datei herunterzuladen. Die E-Mails können auch gefälschte Links zu legitimen Websites enthalten, um den Anschein zu erwecken, dass sie sicher sind.

Die Folgen von Spear-Phishing-Angriffen können schwerwiegend sein, da sie oft darauf abzielen, vertrauliche Informationen wie Benutzernamen und Passwörter, Kreditkarteninformationen oder andere sensible Daten zu stehlen. Diese Informationen können dann für Identitätsdiebstahl oder andere kriminelle Aktivitäten verwendet werden. Unternehmen können auch finanzielle Verluste erleiden, wenn sensible Geschäftsdaten oder Finanzinformationen gestohlen werden.

Spoofing bezieht sich auf eine Technik, bei der ein Angreifer seine Identität oder Herkunft verschleiert, um sich als jemand anderes auszugeben und so unautorisierten Zugriff auf ein Netzwerk, einen Computer oder ein System zu erlangen. Spoofing kann auf verschiedene Arten durchgeführt werden, einschließlich IP-Spoofing, E-Mail-Spoofing, URL-Spoofing und Caller-ID-Spoofing.

IP-Spoofing ist eine Methode, bei der ein Angreifer eine gefälschte IP-Adresse verwendet, um sich als ein anderes Gerät auszugeben und dadurch unautorisierten Zugriff auf ein Netzwerk zu erhalten. Dadurch kann der Angreifer beispielsweise die Absender-Adresse seiner gesendeten Datenpakete manipulieren. Dies kann er dann zur Vorbereitung bzw. Durchführung weiterer Angriffe nutzen.

E-Mail Spoofing ist eine Technik, bei der ein Angreifer seine E-Mail-Adresse fälscht, um sich als jemand anderes auszugeben, z.B. als eine vertrauenswürdige Person oder ein Unternehmen. Dadurch kann der / die Angreifer*in Phishing-E-Mails verschicken oder Malware an Empfänger senden, um Zugriff auf ihre Computer oder Netzwerke zu erlangen.

URL-Spoofing bezieht sich auf eine Methode, bei der ein Angreifer eine gefälschte URL erstellt, um Benutzer dazu zu verleiten, eine gefälschte Website zu besuchen, die wie eine legitime Website aussieht. Dadurch kann der Angreifer versuchen, Benutzer dazu zu bringen, vertrauliche Informationen wie Passwörter oder Kreditkarteninformationen preiszugeben.

Caller-ID-Spoofing ist eine Technik, bei der ein Angreifer die Rufnummer ändert, die auf dem Display des Empfängers angezeigt wird, wenn er einen Anruf tätigt. Dadurch kann der Angreifer vorgeben, von einer vertrauenswürdigen Quelle zu stammen, um den Empfänger dazu zu bringen, vertrauliche Informationen preiszugeben oder unautorisierten Zugriff auf ein Netzwerk oder System zu gewähren.

Sniffing bezieht sich auf die Praxis des Abfangens und Überwachens von Netzwerkdatenverkehr, um vertrauliche Informationen wie Benutzernamen, Passwörter und andere persönliche Daten zu stehlen. Ein Sniffer ist eine Software- oder Hardwarekomponente, die in der Lage ist, Netzwerkdaten zu analysieren und zu erfassen, indem sie den Datenverkehr zwischen Computern oder Netzwerkgeräten abhört.

Sniffing-Angriffe können auf verschiedene Weise durchgeführt werden, wie z.B. durch den Einsatz von Software-basierten Sniffern oder durch den Einsatz von Hardware-basierten Geräten, die speziell für diesen Zweck entwickelt wurden. Einige Sniffer können auch verwendet werden, um Daten in Echtzeit zu analysieren und an einen Angreifer weiterzuleiten.

DoS/ DDoS Denial-of-Service (DoS) ist eine Art von Cyberangriff, bei dem ein Angreifer versucht, eine Website, einen Server oder ein Netzwerk unzugänglich zu machen, indem er es mit einer Vielzahl von Anfragen oder Datenpaketen überflutet, um es zu überlasten. Das Ergebnis ist, dass legitime Nutzer*innen nicht in der Lage sind, auf den Dienst zuzugreifen oder ihn zu nutzen.

Ein DoS-Angriff kann auf verschiedene Weise durchgeführt werden, wie z.B. durch den Einsatz von Botnets, die aus Tausenden von infizierten Computern bestehen und ferngesteuert werden können, um Anfragen oder Datenpakete zu senden, oder durch den Einsatz von speziell entwickelter Malware, die eine Überlastung des Zielsystems verursachen kann.

Eine erweiterte Version von DoS ist DDoS (Distributed Denial-of-Service), bei dem ein Angreifer eine große Anzahl von Computern oder Geräten verwendet, die in der Regel Teil eines Botnets sind, um das Ziel mit einer noch viel größeren Anzahl von Anfragen oder Datenpaketen zu überfluten.

Man in the Middle "Man in the middle" (MITM) ist eine Art von Angriff auf die Netzwerksicherheit, bei dem ein Angreifer sich zwischen zwei Kommunikationsparteien in einem Netzwerk positioniert und den Datenverkehr abfängt, abhört und manipuliert. Der Angreifer kann dabei die gesamte Kommunikation zwischen den beiden Parteien lesen, ändern oder sogar blockieren, ohne dass die betroffenen Parteien es bemerken.

Ein Beispiel dafür ist, wenn ein Angreifer sich zwischen einem Computer und dem Router positioniert, um den Datenverkehr zwischen dem Computer und dem Internet abzufangen. Der Angreifer kann dann die Daten lesen und manipulieren, bevor sie zum Router und zurück zum Computer gelangen.

Bruteforce ist eine Methode, die von Angreifern eingesetzt wird, um Passwörter oder Verschlüsselungsschlüssel zu erraten, indem sie systematisch und automatisch alle möglichen Kombinationen von Zeichen ausprobieren, bis sie die richtige Kombination gefunden haben.

Diese Methode ist insbesondere bei schlecht gewählten Passwörtern oder schwachen Verschlüsselungen effektiv, da sie Angreifer*innen ermöglicht, in kurzer Zeit große Mengen von Passwortkombinationen auszuprobieren. In der Regel werden Programme oder Skripte verwendet, um diese Angriffe durchzuführen, da es sehr zeitaufwändig und ineffizient ist, dies manuell zu tun.

Bruteforce-Angriffe können auf verschiedene Arten durchgeführt werden, zum Beispiel durch das Ausprobieren von Passwörtern auf einer Website, indem sie mehrere Anmeldungen hintereinander durchführen oder indem sie auf verschlüsselte Dateien oder Datenbanken zugreifen.

Keylogger: Ein Keylogger ist eine Art von Malware oder Hardware-Gerät, das die Tastatureingaben eines Benutzers aufzeichnet und speichert. Es kann verwendet werden, um Benutzeraktivitäten zu überwachen, Benutzerinformationen wie Benutzernamen, Passwörter und Kreditkartennummern zu stehlen oder den Benutzer in Echtzeit zu überwachen.

Keylogger können auf verschiedene Arten implementiert werden. Einige sind in Software eingebettet, die auf einem infizierten Computer installiert wird, während andere als Hardware-Geräte installiert werden, die zwischen der Tastatur und dem Computer angeschlossen sind. Einige Keylogger können auch in der Lage sein, Screenshots zu machen oder die Webcam zu aktivieren, um Videoaufnahmen des Benutzers zu machen. Mithilfe von Maschinellem Lernen und Künstlicher Intelligenz kann es zudem sogar möglich sein anhand der Geräusche einer Tastatur die eingegebenen Zeichen zu erkennen.

Keylogger sind sehr gefährlich, da sie den Angreifern den Zugriff auf alle Arten von vertraulichen Informationen ermöglichen können.

Einige Anwendungsbeispiele von Keyloggern können sein:

- Überwachung von Mitarbeiteraktivitäten am Arbeitsplatz
- Identitätsdiebstahl durch die Aufzeichnung von Benutzernamen, Passwörtern und Kreditkartennummern
- Überwachung des Online-Verhaltens von Benutzern für Marketingzwecke

Das MORGENSTERN Magazin

the future is yours.

MORGENSTERN consecom GmbH
Große Himmelsgasse 1
DE - 67346 Speyer

Telefon
+49 (0) 6232 - 100119 44

E-Mail
contact@morgenstern-privacy.com

Passende Weiterbildungen finden Sie hier:

Weiterbildung zum Thema Recht

Finden Sie aus unserem breiten, erstklassigen Weiterbildungsangebot die für Ihre Bedürfnisse passende Fortbildung. Profitieren Sie von unseren maßgeschneiderten Seminaren und Lehrgängen mit erfahrenen, hochkarätigen Experten rund um das Thema Recht. Jetzt informieren.

e-Learning – Klicken und Lernen

Das FORUM Institut bietet mit hochwertigen e-Learning-Programmen eine flexible Weiterbildungsform. Entscheiden Sie selbst, wann und wo Sie lernen.
Jetzt testen.

Inhouse-Seminare – Maßgeschneiderte Lösungen

Alle unsere Seminare eignen sich auch hervorragend als Inhouse-Training.
Jetzt individuelles Angebot anfordern.

Dieses Whitepaper wurde Ihnen von unserem Content-Partner präsentiert.
sichern Sie sich jetzt eine individuelle und zielgenaue Beratung.

MORGENSTERN legal | Dein Partner in Sachen IT-Recht & Digitalisierung
morgenstern-legal.com

MORGENSTERN privacy | Dein Partner in Sachen Datenschutz & IT-Sicherheit
morgenstern-privacy.com

FORUM · Institut für Management GmbH · Postfach 10 50 60 · 69040 Heidelberg · Germany
Tel. +49 6221 500-500 · Fax +49 6221 500-555 · www.forum-institut.de