Individuelle Security-Konzepte.

Wir unterstützen Sie im Kampf gegen Cyberkriminalität.

Informieren Sie sich jetzt!
security.doh.de

Seite 04 — Threat Protection

Seite 06 — Incident Response

Seite 08 — Penetration Tests

Seite 10 — Security Services

ALLE LÖSUNGEN AUF EINEN BLICK

Wir geben Hackern **keine Chance.**

Cyberangriffe gibt es immer häufiger und zumeist beschäftigen sich Unternehmen erst mit dem Thema, wenn es zu spät ist und Ihr Image darunter leidet. Wir erstellen gemeinsam mit Ihnen etablierte Sicherungs- und Wiederherstellungskonzepte, bevor dieser Fall eintritt.

Sicherheit geht vor.

Zu den beliebtesten cyberkriminellen Methoden gehört die sogenannte Ransomware, da sie immense (finanzielle) Schäden bei den Opfern anrichten und somit große Gewinne erzielt werden können.

Unternehmensvertrauliche Dienste und Dateien werden verschlüsselt und nur gegen ein Lösegeld in Form von Bitcoins freigegeben. Dabei ist es nicht immer klar, ob die Freigabe der Daten im Anschluss auch tatsächlich erfolgt. Große Unternehmen, staatliche Einrichtungen sowie kritische Infrastrukturen sind hierbei begehrte Ziele für die Hacker. Erhebliche Einsatzbußen bis hin zu einer Insolvenz sind die schlimmsten Auswirkungen eines Angriffs.

Durch die Kombination von mehreren Malwarearten und das Eindringen an unterschiedlichsten Schwachstellen werden Cyberangriffe zunehmend komplexer und sind dadurch auch schwieriger zu erkennen. Als eine der größten Sicherheitslücken in einem Unternehmen gilt immer noch der Mensch vor dem PC. Hacker schlüpfen somit in die Rolle einer Person aus der Führungsebene und versenden gefälschte E-Mails an Mitarbeiter – oftmals mit der Bitte, große Geldbeträge zu überweisen. Um Druck aufzubauen und eine schnelle Überweisung zu veranlassen, werden im Vorfeld Informationen über Vertragsverhandlungen oder Auslandsreisen ausgespäht, um so das Vertrauen des Mitarbeiters zu gewinnen.

Damit Bedrohungen und alle Eventualitäten von Ihrer IT-Infrastruktur ferngehalten werden, kombinieren und beherrschen wir eine Vielzahl an Methoden sowie Abwehrmechanismen. Wir bauen Ihnen somit ein sicheres Schutzschild um Ihre Dienste und Daten. //

ESSENZIELL

Threat Protection.

- Ransomware Protection
- Network Security
- Endpoint Security
- Encryption
- E-Mail Security
- App Security
- Cloud Security

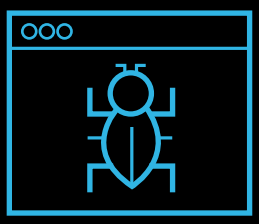
AKUT

Incident Response.

- Endpoint Detection & Response (EDR)
- Extended Detection & Response (XDR)
- Health Checks
- Managed Response

PROAKTIV

Penetration Tests.



- Social Engineering
- Systemanalyse
- Network / Wifi
- Webapplikation
- Workflow
- Physical Security
- Threat Hunting

Auf in die Tiefen **Ihres Netzwerks.**

Bei der Threat Protection erkennen, analysieren und verhindern wir vielseitige Bedrohungen in Form von Malware, die kontinuierlich weiterentwickelt wird, um herkömmliche Sicherheitsmethoden zu umgehen. Wir beheben Schwachstellen in den Netzwerken von heute und erweitern stetig unser Repertoire, um beste Sicherheitsvorkehrungen für Ihre IT-Infrastruktur zu schaffen.

Threat Protection Services.

Ransomware Protection

Alle 11 Sekunden wird ein Unternehmen Zielscheibe eines Ransomware Angriffs. Durch Schwachstellen in Software und Systemen oder durch unvorsichtiges menschliches Verhalten bekommen Hacker Zugriff auf die Endpunkte eines Unternehmens. Ransomware übernimmt die Kontrolle über den Computer, das Gerät oder die Daten und der normale Zugriff wird erst gegen Zahlung eines Lösegelds wiederhergestellt. Je nach Größe des Unternehmens variieren auch die Störungen des Betriebs, die Wiederherstellungskosten oder die potenziellen Langzeitschäden. Wir bieten branchenführende Lösungen für Bedrohungsüberwachung, Datensicherung und -wiederherstellung.

Network Security

Durch die hohe Dynamik der Geschäftsprozesse ist eine kontinuierliche Optimierung der Network Security unumgänglich. Weiterentwicklungen wie Virtualisierung von Server-Systemen müssen stetig an die Infrastruktur und aktuellen Anforderungen angepasst werden. Internetverbindungen und Übergänge zwischen Unternehmensbereichen sind Netzwerkübergänge, die von Firewalls streng kontrolliert werden müssen. Damit werden alle Dienste und Daten vor unberechtigten Zugriffen geschützt. Aufgrund von unterschiedlichen Regeln und Voraussetzungen eines jeden Unternehmens sollten die Firewall-Lösungen stets individuell angepasst werden. Nur so kann eine Netzwerksicherheit auf hohem Level gewährleistet werden.

Endpoint Security

Entpoint Security hat in den letzten Jahren durch die Digitalisierung intensiv an Bedeutung gewonnen, da die Anzahl an Endgeräten, die in einem Unternehmensnetzwerk kommunizieren, stetig zunimmt. Mit der steigenden Beliebtheit von Modellen wie „Bring Your Own Device" und dem „Internet der Dinge – IoT" kann die Zahl, der mit dem Unternehmensnetzwerk verbundenen Geräte, schnell in die Zehn- und Hunderttausende gehen. Endgeräte und vor allem Remote- sowie Mobilgeräte sind ein sehr beliebtes Angriffsziel, da sie als größte Eintrittsstelle gelten. Durch mehrschichtige Ansätze wie Deep-Learning-KI, Anti-Ransomware-Funktionen und Exploit Prevention kombinieren wir moderne und traditionelle Techniken, um die unterschiedlichsten Bedrohungen zu stoppen.

Encryption

Aufgrund der steigenden Tendenz zum Home-Office ist es umso wichtiger, einen Schutz Ihrer Daten auf verschiedenen Geräten zu gewährleisten. Hierbei kommt eine spezielle validierte Verschlüsselungslösung (DSGVO-konform) zum Einsatz. Alle Daten werden vollständig verschlüsselt, um die Kompromittierung vertraulicher Daten zu verhindern, insbesondere durch gestohlene oder verloren gegangene Geräte. Sämtliche Daten und Dateien sind für unbefugte Personen nun unleserlich und damit unbrauchbar.

Wir sind Experten, die immer auf dem neusten Stand sind.

E-Mail Security

Mit zu den am wichtigsten, aber leider auch am unsichersten Kommunikationsmitteln gehören heutzutage E-Mails. Diese werden im Normalfall unverschlüsselt über ein Netzwerk übertragen und geben somit eine schnelle und einfache Angriffsfläche für Hacker ab. Um Malware, Phishing-Links und Ähnliches abzuwehren, stellen wir dedizierte Sicherheitsprodukte zur Verfügung, die sich ausschließlich dem Absichern des Mail-Verkehrs widmen. Wir konfigurieren maßgeschneiderte Richtlinien, die sich Ihrer Unternehmensstruktur anpassen und definieren eine automatisierte Maßnahme zur Bedrohungsabwehr.

App Security

Um das Risikopotenzial Ihrer mobilen Apps auszuwerten und den Schutz Ihrer mobilen Geräte sicherzustellen, bieten wir einen ganzheitlichen Service im Bereich App Security Lösungen an. Wir analysieren Schwachstellen und identifizieren riskantes Verhalten, unzulässige Verbindungen und Datenübertragungen zu Dritten werden genauestens unter die Lupe genommen. Erhalten auch Sie einen schnellen Viren-, Phishing- und Mobilschutz für alle öffentlichen und betriebsinternen Apps der führenden Betriebssysteme sowie für Ihre Geräte.

Cloud Security

Da wir heute enger vernetzt sind als je zuvor, umfasst unsere Cloud Security eine breite Palette von Technologien, Richtlinien und Anwendungen, um wichtige Daten vor Hacker Angriffen zu schützen. Dadurch können eine Ausbreitung von Malware auf das Netzwerk verhindert werden und wichtige Daten von Benutzern sowie Dateien gesichert werden. Darüber hinaus überwachen wir Sie und informieren Sie über verdächtige Aktivitäten, um so ein angemessenes Sicherheitsniveau für Ihre Endbenutzer gewährleisten zu können. //

DIE WICHTIGSTEN MASSNAHMEN

Unsere Soforthilfe **bei Cyber-Notfällen.**

Sollte bei Ihnen ein Verdacht auf einen Angriff vorliegen, zögern Sie nicht, uns sofort zu kontaktieren.

Wir mobilisieren sofort unsere spezialisierten Cyberexperten und schauen bei Ihnen vor Ort, ob es sich wirklich um einen Cyberangriff handelt. Mit unseren organisatorischen und technischen Tools sind wir bestens ausgestattet, um Ihre Daten und Dateien, wenn nötig auch in unserer eigenen DOH-Cloud, zu sichern. Dabei ist es egal, ob es sich um eine einzelne Applikation wie ein Personalsystem handelt oder um komplette IT-Landschaften. Durch eine anschließende Analyse können wir genauesten das Ausmaß und die Art des Angriffs ermitteln und so eine Ausarbeitung von Lösungskonzepten bereitstellen. Ihr System kann nun gezielt gereinigt, überwacht und vor neuen Angriffen geschützt werden. Es besteht auch die Möglichkeit, es neu und sicher aufzubauen, damit alte Daten sauber wiederhergestellt werden können.

Prävention statt **Schadensbehebung.**

Weil auch Ihr Unternehmen leicht ins Visier eines Hackers gelangen kann, ist es umso wichtiger, sich für den Ernstfall eines Angriffs zu rüsten. Je schneller man bei einem Vorfall reagieren kann, desto höher ist die Chance, einen Datendiebstahl oder die Verschlüsselung Ihrer Systeme zu verhindern.

Incident Response Services.

Endpoint Detection & Response

Als Endpoint Detection & Response, kurz EDR, werden Security Lösungen bezeichnet, die sich von Anderen unterscheiden, indem sie direkten Schutz auf Ihren Endgeräten bieten. Es werden große Datenmengen kontextbezogen und in Echtzeit analysiert, ähnlich einer Blackbox in einem Passagierflugzeug. Somit erkennen sie potenziell verdächtige Aktivitäten auf PCs, Laptops und anderen Geräten eines Unternehmens und reagieren gezielt darauf. Durch die Echtzeitalarme können Angriffe frühzeitig erkannt werden und verschiedene Maßnahmen ergriffen werden, um ein größeres Datenleck zu verhindern.

Extended Detection & Response

Der Nachfolger von EDR ist die Extended Detection & Response, auch XDR genannt. Im Gegensatz zu EDR kombiniert XDR die Daten aus allen IT-Schichten und bezieht somit sowohl Ihre Server, Netzwerke, Anwendungen als auch Cloud-Services mit ein. Dank der integrierten Analysefunktionen bringt es schneller unterschiedliche Aspekte zusammen und liefert ein vollständigeres Bild des Cyberangriffs, welches so besser und schneller abgeblockt werden kann. Zusätzlich können Angriffe zurückverfolgt und einfacher rekonstruiert werden.

Health Checks

Fachliche und technische Anforderungen müssen korrekt umgesetzt sein, damit eine Anwendung erfolgreich betrieben werden kann. Hierzu gehören die Health Checks. Sie sind sowohl für Menschen als auch für Maschinen entwickelt worden. Hierbei geht es um keine fehlerhaften Eingaben, sondern vielmehr um Probleme mit externen Ressourcen wie z. B. Datenbanken, Festplatten, Verbindungen zu Systemen und anderen Anwendungen. Es wird den Mitarbeitern ermöglicht, im Fehlerfall auf einen Blick zu erkennen, wo dieser entstanden sein könnte. Auch Maschinen können automatisch entscheiden, ob eine Instanz der Anwendung noch verwendbar ist. Dadurch können einzelne Instanzen einfach gestoppt oder, falls nötig, auch neu gestartet werden.

Managed Detection & Response

Unsere Managed Detection and Response Services überwachen Sie rund um die Uhr und schützen Sie somit vor Bedrohungen und erledigen die Abwehr von Angriffen. In Ihrer Systemumgebung werden leistungsstarke Methoden eingesetzt, um menschliche Bedrohungen zu erkennen und die Quellen des Übels zu entlarven. Eine abgestimmte Beratung mit einer detaillierten Berichterstattung dämmt alle Risiken ein und behebt automatisiert Ihre Schwachstellen. Zudem ermöglichen wir in unserem Service Implementierungen auf Grundlage Ihrer spezifischen Bedürfnisse. Wenn wir ein Risiko erkennen, geben wir Ihnen nicht nur einen Hinweis, sondern sind auch bei Lösungen behilflich. //

In der Rolle eines Hackers.

Um das Angriffspotenzial auf Ihr IT-Netz, ihr IT-System oder auf eine Anwendung einzuschätzen, führen wir erprobte Penetrationstests durch. Somit versetzen wir uns in die Rolle eines Hackers und versuchen mit vorsätzlich durchgeführten Angriffen an die Daten Ihres Unternehmens zu gelangen. Es werden alle IT-Anwendungen, Betriebssysteme, Datenbanken u. Ä. mit unterschiedlichen Tests in Umfang und Aggressivität überprüft. Durch die nachfolgenden Testergebnisse können wir einschätzen, ob die bereits umgesetzten Sicherheitsmaßnahmen ausreichen oder ob zusätzliche Sicherheitsmaßnahmen eingeleitet werden müssen. IT-Penetrationstests müssen an jede Umgebung und Gegebenheiten flexibel angepasst und durchgeführt werden. Gemeinsam entscheiden wir, welche Penetrationstests sinnvoll sind und welches Risiko für Sie tragbar ist.

Penetration Tests.

- Social Engineering
- Systemanalyse
- Network / Wifi
- Webapplikation
- Workflow
- Physical Security
- Threat Hunting

Social Engineering

Social Engineering findet leider nicht nur im Internet statt, sondern ist schon eine seit Jahrzehnten erprobte Masche, bei dem der Cyberkriminelle versucht, das Vertrauen des Opfers zu gewinnen und ihn so dazu bewegt, vertrauliche Informationen freizugeben oder Kreditkartendaten sowie Passwörter zu veröffentlichen. Der für Privatpersonen bekannteste Trick ist der Enkel-Trick, bei dem Betrüger sich über Telefonanrufe bei älteren Menschen melden und versuchen sich als Verwandter oder Enkel auszugeben, um so an Geld zu gelangen. Das größere Ziel, mit dem oftmals höhere Beträge erbeutet werden können, sind Unternehmen. Das Vorgehen verläuft allerdings sehr ähnlich wie bei einer Privatperson, nimmt aber bedeutend mehr Zeit in Anspruch. Eine gefälschte E-Mail Adresse, ähnlich die eines Vorgesetzten, ist hier der einfachste Weg, Mitarbeiter mit einem dringenden Anliegen dazu zu bewegen, größere Geldbeträge zu überweisen – ganz ohne Rückfragen. Regelmäßige Schulungen für Ihre Mitarbeiter können helfen, Aufmerksamkeit und Achtsamkeit zu steigern, sowie sie für gefälschte E-Mails zu sensibilisieren. Zusätzlich werden spezielle Spamfilter eingesetzt, die ungewollte E-Mails sofort erkennen und aussortieren.

Network / Wifi

Die Nutzung von WLAN ist in der heutigen Zeit kaum wegzudenken. Immer mehr mobile Computer und IoT-Devices werden in Unternehmen eingebunden und somit steigt die Angriffsfläche für Hacker und Cyberkriminelle um ein Vielfaches an. Im Gegensatz zu kabelgebundenen Netzwerken, die innerhalb Ihres Gebäudes verlaufen und den Datenabgriff erheblich erschweren, sind die kabellosen Netzwerke durch Abgabe eines Funksignales in einen freien Raum deutlich unsicherer und leichter abzufangen. Wir bieten Ihnen eine sichere und kundenspezifische

Entwicklung eines Gesamtkonzeptes für Ihr Netzwerk. Dabei ist das spezielle Anforderungsprofil Ihres Unternehmens der Ausgangspunkt für alle Überlegungen und Sicherheitslösungen.

Webapplication

Alle Webanwendungen stellen aufgrund ihrer öffentlichen Erreichbarkeit ein weiteres beliebtes Ziel für Angreifer dar. Das Risiko wird durch ihre Komplexität und Verbindungen zu anderen Systemen wie Datenbanken deutlich erhöht. Wir überprüfen mit Penetrationstests das Frontend, das Backend, die Datenbanken und alle möglichen Schnittstellen auf Schwachstellen. Des Weiteren setzen wir sowohl spezifische, manuelle Analysen wie auch automatische Scans ein, um gezielt Insuffizienzen zu finden. Somit werden alle Sicherheitslücken gefunden und behoben, bevor Andere sie ausnutzen können.

Physical Security

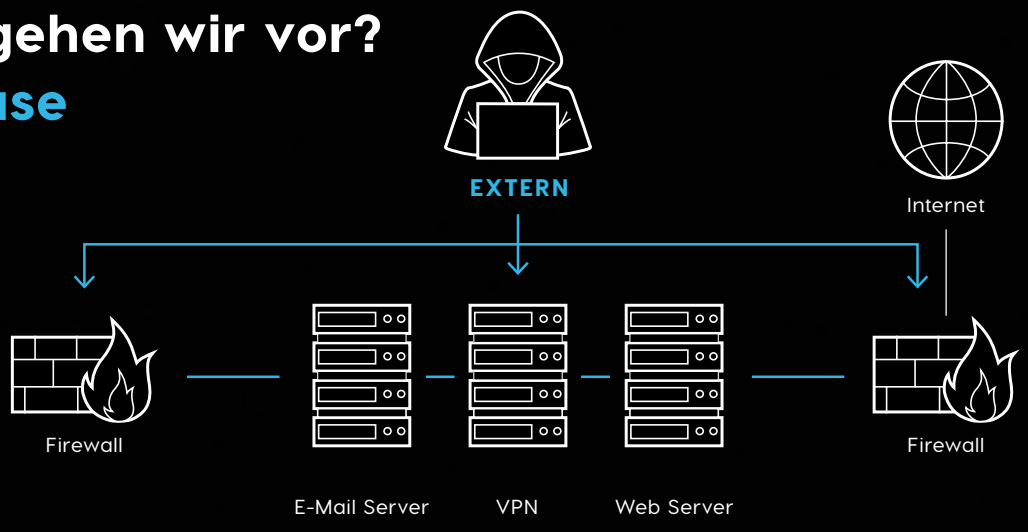
Eins der unterschätztesten Sicherheitsaufgaben ist die physische Sicherheit. Viele Unternehmen ergreifen technische Maßnahmen, um einen Angriff abzuwehren, allerdings wird dabei immer wieder das eigene Rechenzentrum oder Gebäude vernachlässigt. Je größer das Unternehmen, umso unüberschaubarer auch die Menschen, die täglich ein- und aus gehen. Das sind dann selten Menschen, die mit dunklen Kapuzenpullis herumlaufen, sondern sie sind oft getarnt als Lieferdienste oder Postboten. Somit können sie sich auf einfachste Weise Zugang in Ihr Gebäude verschaffen und schnellstens Daten stehlen, die Ihre IT-Technik dauerhaft schädigen können. Wir testen genau diesen unberechtigten Zugang auf Ihr Gelände und prüfen alle weiteren physischen Schwachstellen wie Zugangs- oder Schließsysteme.

Threat Hunting

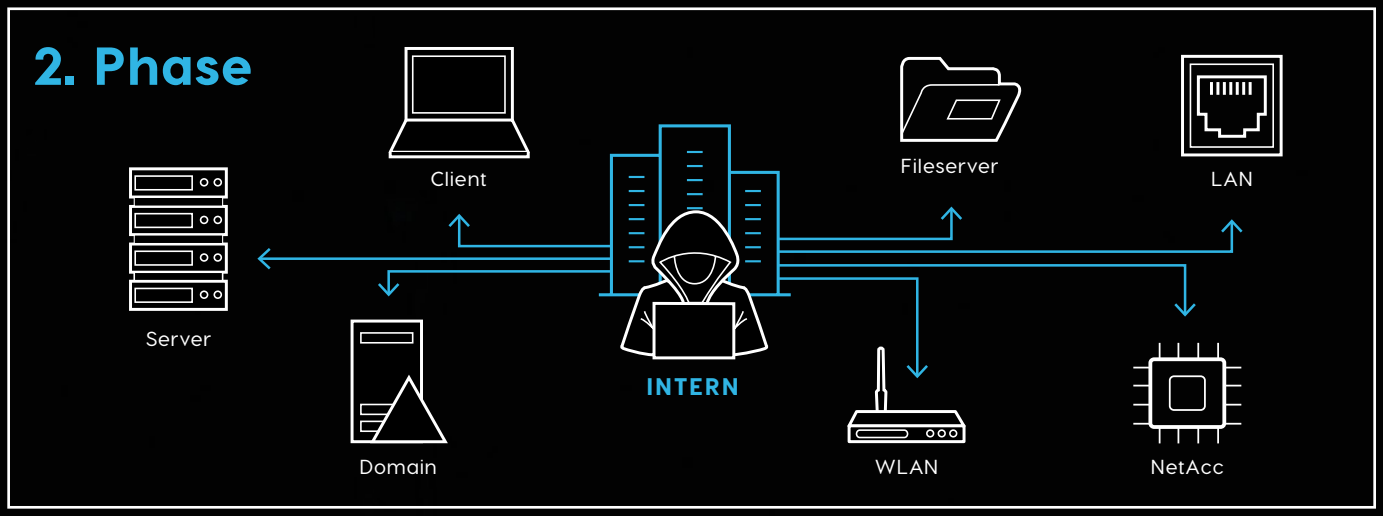
Beim Threat Hunting handelt es sich um eine Bedrohungssuche, die proaktiv – also ohne konkrete Anzeichen für einen Angriff – durchgeführt wird. Durchforstet wird Ihr Netzwerk oder Ihre IT-Systeme von einem speziell zugewiesenen Sicherheitsexperten, der die Prozesse teils manuell durchführt. Unterstützt wird dieser von vielen automatisierten Techniken oder bestimmten Tools, die in der Lage sind, große Datenmengen nach Anomalien und verdächtigen Verhaltensmustern zu durchsuchen. Aufgrund dieses Verfahrens können auch Angreifer gefunden werden, die sich bereits Zugriff verschafft haben, aber sich aktuell noch still verhalten. Somit kann sich niemand unbemerkt in Ihrer IT-Umgebung aufhalten und Schäden anrichten. //

Wie gehen wir vor?

1. Phase



2. Phase



Unsere Service-Modelle **für Ihre Sicherheit.**

Unsere Service-Modelle sind hochflexibel und genauestens auf Ihr Unternehmen und Ihre Herausforderungen angepasst. Ob kleinere Unternehmen oder Großkonzerne – wir gehen auf Ihre individuellen Anforderungen ein und sind Ihr zuverlässiger IT-Partner!

BASIC

☆

Perfekt vorgesorgt.

Zum Schutz Ihrer Daten und Systeme bieten wir Ihnen mit dem Basic-Modell eine elementare und unerlässliche Grundausstattung.

PREMIUM

☆☆

Ganzheitlich geschützt.

Entscheiden Sie sich jetzt für unsere Premium-Variante und genießen Sie die vielen Vorteile unserer Security-Dienstleistungen.

EXTENDED

☆☆☆

Zusätzlich abgesichert.

Besser geht´s nicht! Unser Extended-Modell bietet Ihnen den besten Schutz vor allen Eventualitäten der Cyberkriminalität.

Entscheiden Sie sich jetzt für eins unserer Security Service-Modelle!

+49 6131.633 81 0 **oder** sales@doh.de

Leistungen im Überblick	BASIC	PREMIUM	EXTENDED
Exklusiver Zugang zum DOH Servicedesk	√	√	√
Kostenloser Austausch bei einem qualifizierten Hardware-Defekt	√	√	√
Monitoring der Secruity-Systeme	X	√	√
Monatliche Kontrolle der Secruity-Systeme (Firmware, Updates, Lizenzen)	X	√	√
Sicherung der Konfigurationsdateien	X	√	√
Monatlicher Scan auf Schwachstellen Ihrer IT-Systeme (Vulnerability Management)	X	√	√
Aufbau einer fortlaufenden Dokumentation	X	X	√
Jährlicher System und Konfigurationscheck	X	X	√
DOH Notfallpass 24/7 Kontakt bei Cyber-Notfällen	X	X	√
Garantierte Reaktionszeiten (Std.)	**keine**	**4/12/48**	**1/8/24**
Inkl. technische Supportanfragen je Monat (Min.)	**0**	**240**	**480**

Zubuchbare Leistungen

Disaster Recovery in die DOH Cloud	+	+	+
Auslagerung Ihres Systems in die DOH Cloud	+	+	+

Wie werden Ihre **Systeme sicher?**

Unser Vorgehen für einen vollen Sicherheitsschutz.

Multi-Faktor-Authentifizierung.

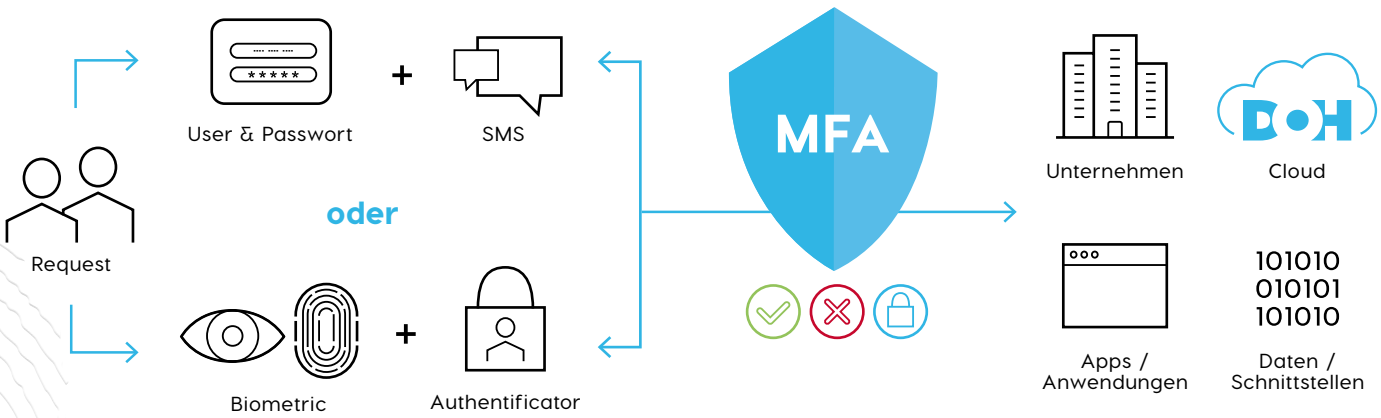
Für einen intelligenten Access.

Um sich ausreichend vor verschiedensten Gefahren zu schützen ist eine Multi-Faktor-Authentifizierung heutzutage essenziell. Hierbei handelt es sich um einen erweiterten Sicherheitsschutz, der durch eine Kombination mehrerer verschiedener und vor allem selbstständiger Identitätsnachweise die Zugänge zu Systemen, Anwendungen und Konten prüft. Somit wird die Sicherheit um ein vielfaches erhöht, denn diese Verfahren können von einem Angreifer nicht ohne Weiteres nachvollzogen oder dupliziert werden. Außerdem sollte auch auf die Komplexität des Sicherheitsverfahrens geachtet werden. Ist die Anmeldung zu komplex, wird damit die Benutzerfreundlichkeit erheblich eingeschränkt und der Mitarbeiter wird sich das Kennwort mit hoher Wahrscheinlichkeit an irgendeiner Stelle notieren. Für einen ausreichenden Sicherheitsschutz bei Ihrem Zugang sind mindestens zwei Authentifizierungsmaßnahmen unumgänglich. Diese Faktoren fallen in drei Kategorien:

Etwas, das Sie wissen. Etwas, das Sie haben und Etwas, das Sie sind.

Unsicher	In Ordnung	Sicher	Am Sichersten
123456 passwort1 ichliebedich passwort Name123	Passwort + SMS oder Voice	Passwort + Push Notification (Authentificator) oder Software Token OTP oder Hardware Token OTP	kein Passwort Biometric + Phone Sign-In (Authentificator) oder Security Key

Wie gehen wir vor?

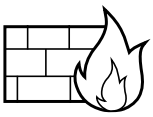


Web-Applikation Firewall.

Angriffe erfolgreich abwehren.

Bei der WAF handelt es sich um eine wichtige Sicherheitskomponente, denn sie arbeitet auf höchster Netzwerkebene und schützt so Ihre Webanwendungen durch Filtern, Überwachen und Blockieren von jeglichem böswilligen Datenverkehr. Sie bietet Schutz vor Angriffen wie Injections, Cross-Site-Scripting und unberechtigte Zugriffe auf Web-Server. Da ein Datenaustausch in diesem Fall gewünscht und meist auch legitim ist, muss hier klar zwischen einer herkömmlichen Firewall und der Web-Application-Firewall unterschieden werden. Im Gegensatz zu einer normalen Firewall, die den Benutzer schützt, schützt die WAF die Anwendungsebene und ist speziell dafür ausgelegt, da sie benutzer-, sitzungs- und anwendungsorientiert filtert. Die Bereitstellung einer WAF kann auf unterschiedlichste Weise erfolgen. Dies hängt von mehreren Faktoren, wie Dienste, Verwaltung, Leistung und Flexibilität ab. Auch eine Kombination von einer herkömmlichen Firewall und einer WAF kommen des öfteren zum Einsatz, da sie in aufeinanderfolgenden Schritten Daten und Kommunikation analysieren.

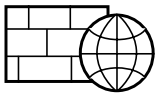
Klassische Firewall.



Klassische Firewalls schützen auf 3. und 4. Netzwerkebene.

- Denial Of Service (Dos)
- SYN Flood
- Distributed DoS
- Ping Of Death
- TCP Session Hijacking
- Packet Fragmentation

Web-Applikation Firewall.



Web-Application-Firewalls schützen 7. Ebene (Anwendungsschicht).

- SQL Injection
- Cross Site Scripting
- Buffer Overflow
- Web Worms
- Cookie Poisoning
- Forceful Browsing

Welche WAF-Arten existieren?

Abhängig von der Positionierung der Firewall unterscheidet man zwischen zwei grundlegenden Architekturen. Denn die WAF kann hinter der Netzwerk Firewall und somit vor dem Webserver (zentralisierte Architektur) platziert werden, als auch direkt auf dem Websever (Host-basierte-Architektur). Bei einer zentralisierten Architektur kommen oft kategorische Geräte zum Einsatz, der Datenverkehr wird hindurchgeleitet bevor sie die Webserver erreichen. Dadurch wird auch eine höhere Leistung benötigt, denn sie muss mehrere Anwendungen gleichzeitig schützen. Bei der Host-basierten-Architektur wird eine zusätzliche Software verwendet, die z. B. Plugins direkt in die Webserver-Software integriert.

Aktiver und passiver Modus.

Des Weiteren unterscheidet man zwischen einem aktiven und passiven Modus der WAF. Bei dem aktiven Modus wird der Netzwerkverkehr aktiv geprüft, unangemessene Vorgänge sofort geblockt oder gelöscht. So wird garantiert, dass unberechtigte Zugriffe die Anwendungsserver erst gar nicht erreichen. Bei dem passiven Modus wird nur die Überwachung und Protokollierung durchgeführt, nicht aber die direkte Reaktion auf den vermeintlich schädlichen Datenverkehr. Sie kann allerdings so konfiguriert werden, dass sie Alarme empfängt oder sendet.

Wie sichern wir Webapplikationen?

» **Schützt Ihre Applikationen vor X-Site Scripting und SQL Injection attacks**

» **Blockiert Bedrohungen auf der Basis von OWASP**

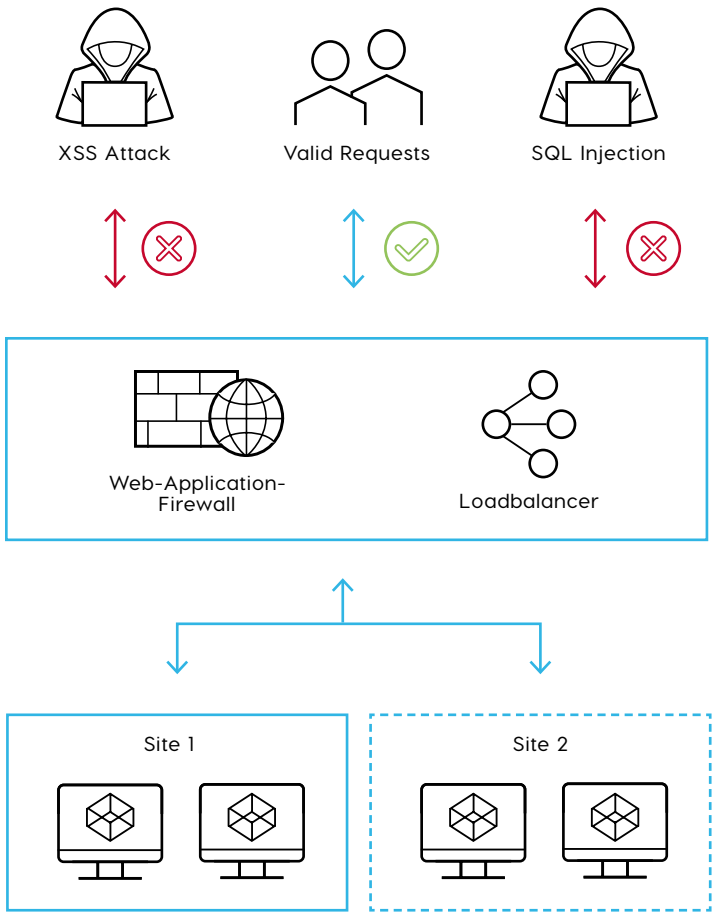
» **Echt-Zeit Protokollierung**

Hohe Verfügbarkeit und Skalierbarkeit
Auch in Public Cloud oder Managedplatt-formen darstellbar

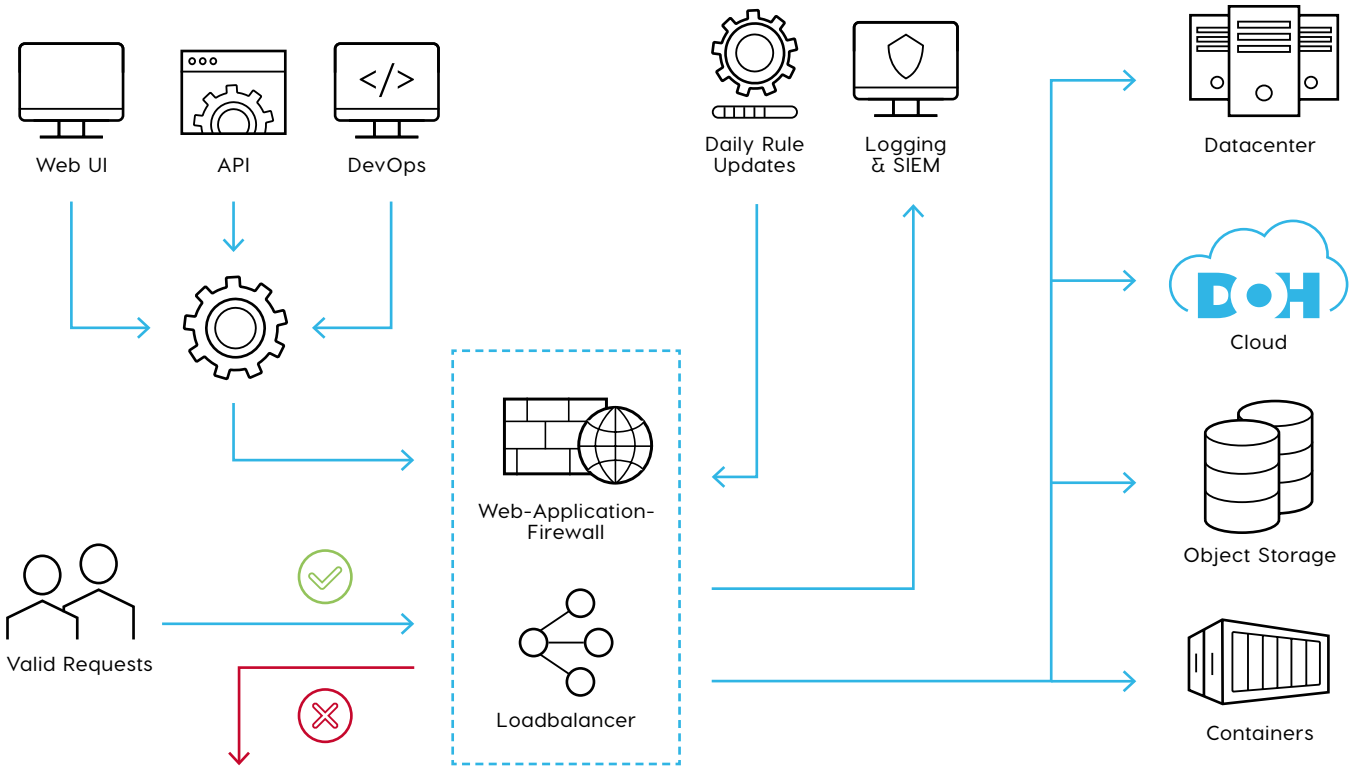
Layer 7 load balancing
URL path, host based, round robin, session affinity, redirection

Zentralisiertes SSL Management
SSL offload und SSL Richtlinien

Überwachung
Monitoring und Log Analysen



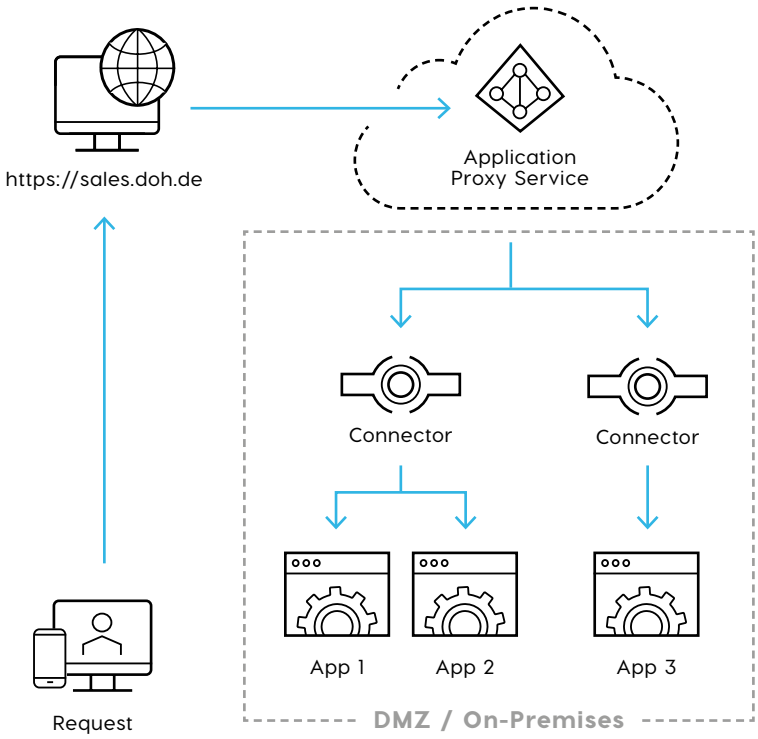
Technisches Schaubild.



Application Proxy.

Außerhalb von Unternehmensgrenzen.

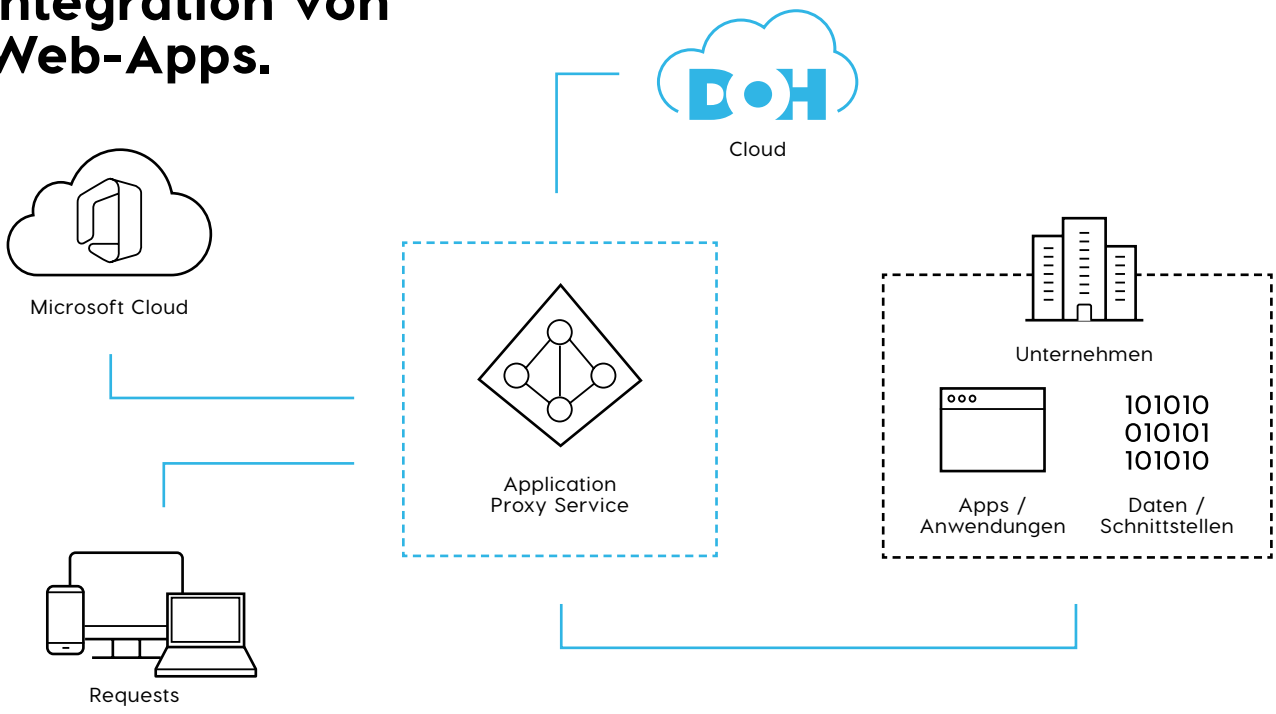
Flexibles Arbeiten wird für viele Menschen zunehmend interessanter und technologisch auch einfacher. Damit verbunden wollen und müssen Unternehmen vermehrt interne Anwendungen schnell und sicher für alle Mitarbeiter von überall aus zur Verfügung stellen. Ein wahrer Juwel in der Mircosoft Azure Cloud ist der Application Proxy, der eine Multi-Faktor-Authentifizierung erzwingen kann und den Zugriff von vertrauten, verwalteten und „gesunden" Geräten sicherstellt. Seine Arbeit umfasst somit ausschließlich ausgehende Netzwerkverbindungen zur Azure Cloud – interne Webseiten bzw. Web-Applikationen können infolgedessen besonders kompakt, sicher und einfach zu administrierend zur Verfügung gestellt werden. Um auf eine Webseite oder eine WebApp zugreifen zu können, kommuniziert der Client ausschließlich mit dem Application Proxy Server, der als Kommunikationsschnittstelle und Abgrenzung dient. Er stellt nun eine Anfrage an den Connector aus dem Firmennetzwerk und bekommt die Erlaubnis erteilt, den Zugriff für den Client freizugeben. Dabei bleibt die wahre Zieladresse des Webservers verborgen. Durch dieses Vorgehen ist eine erhöhte Sicherheit gewährleistet, denn der Client hat keinen direkten Zugriff auf den firmeninternen Server.



Authentifizierungsprotokolle

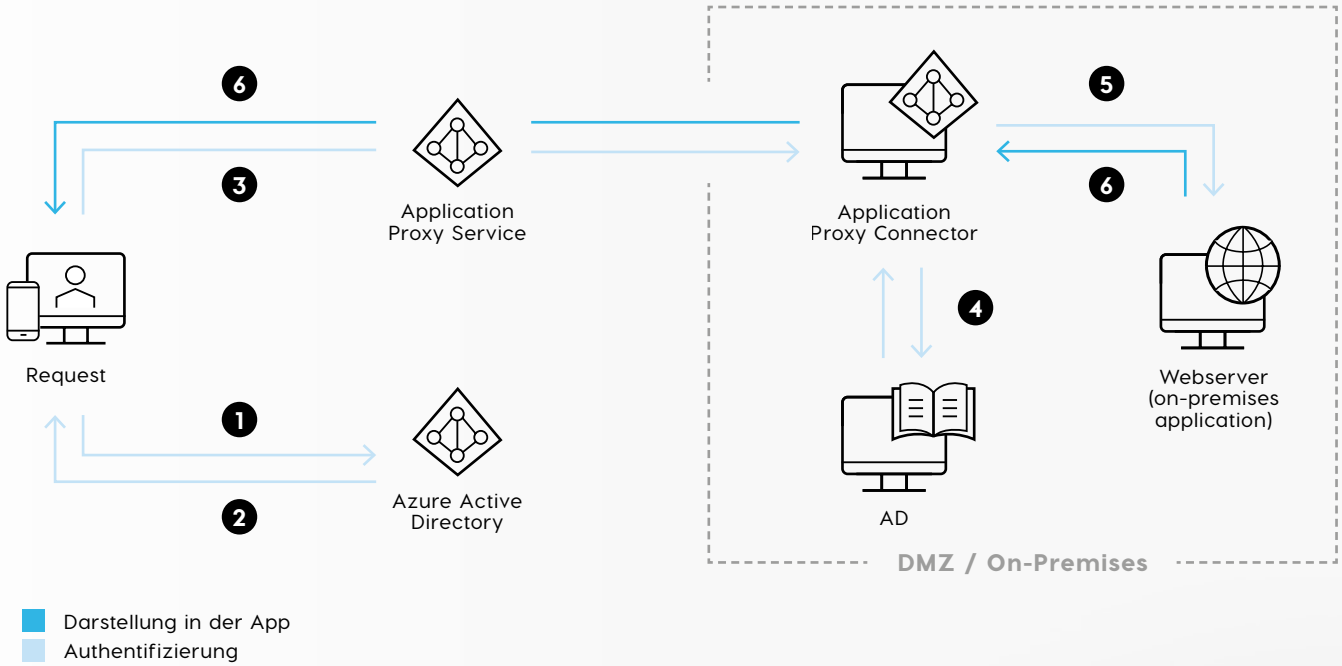
- **Headerbasiert**
- **Formular- oder kennwortbasiert**
- **SAML-basiert**

Integration von Web-Apps.



Bereitstellung der Anmeldung bei lokalen Anwendungen.

Dieses Diagramm zeigt wie Azure AD und der Anwendungsproxy gemeinsam das einmalige Anmelden für lokale Anwendungen bereitstellen.



Darstellung in der App
Authentifizierung

Erklärung der Funktionsweise.

1. Zugriff auf die Anwendung über den Application Proxy Service und Weiterleitung zur Azure AD Anmeldeseite für die Authentifizierung. (Möglich sind SSO mit Corporate Device; SSO für interne Anwender, alle Azure AD Authentifizierungsmethoden, wie Föderation mit ADFS oder Passthrough etc...)
2. Nach erfolgreicher Anmeldung wird ein Token generiert und dem Client Device vermittelt.
3. Token wird zum Application Proxy Service vermittelt, der den User Principal Name (UPN) und den Security Principal Name (SPN) des Tokens ausliest, um daraufhin die Anfrage an den Application Proxy Connector zu leiten.
4. Bei konfiguriertem Single-Sign-On kümmert sich der Connector um die weiteren für den User nötigen Authentifizierungen.
5. Der Connector sendet die Anfrage zur On-Prem-Application.
6. Die Antwort wird über den Application Proxy Service und den Connector zum User geschickt.

Gender-Hinweis: Aus Gründen der besseren Lesbarkeit wird in dieser Broschüre die Sprachform des generischen Maskulinums angewendet. Es wird an dieser Stelle darauf hingewiesen, dass die ausschließliche Verwendung der männlichen Form geschlechtsunabhängig verstanden werden soll.

IN DER WELT DER DIGITALISIERUNG

Gemeinsam alle **Ziele erreichen.**

Als strategischer IT-Partner für Cloud-Plattformen unterstützen und begleiten wir Sie auf dem Weg Ihrer digitalen Roadmap. Unsere Aufgabe besteht darin, Ihre IT-Infrastruktur an den permanenten Wandel anzupassen und zu ergänzen, während Sie sich weiterhin auf Ihre Kerngeschäfte fokussieren.

DOH CLOUD

Die Zukunft Ihrer modernen IT liegt in unserer Cloud.

CONSULTING

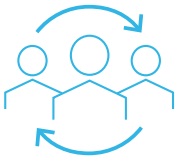
Beratung und Unterstützung in eine digitale Zukunft.

IT-SERVICES

IT-Dienstleistungen für Ihre individuellen Bedürfnisse.

BESCHAFFUNG

IT-Beschaffung für alle Unternehmensbereiche.



APP-SERVICES

Ihr Wegbegleiter für ein digitales Business.

DEVELOPMENT

Umwandlung Ihrer Ideen als digitale Softwareprodukte.

Kennen Sie schon unsere Webseite?
www.doh.de

Unsere Security Partner.

SOPHOS · VEEAM · kemp · Microsoft · Greenbone · HORNETSECURITY

DOH GmbH
Taunusstraße 57
D-55118 Mainz
+49 6131.633 81 0
info@doh.de
www.doh.de