alphasolid
PASSION TO PERFORM IT

Stay Solid.

Das Alphasolid Portfolio für Ihre IT-Sicherheit

Die Sicherheit Ihrer IT-Systeme ist nicht verhandelbar.

Kontaktieren Sie uns: +49 5932 500981 8 sales@alphasolid.de **alphasolid.de**

Wir bieten Ihnen ein umfassendes Portfolio, das alle Aspekte der Cybersecurity abdeckt – von der **Analyse** über den **Schutz** bis zur **Sensibilisierung** Ihrer Mitarbeiter. Ob Penetrationstests, AD-Härtung oder kontinuierliches Monitoring:

Wir sorgen dafür, dass Ihre IT-Infrastruktur bestmöglich geschützt ist.

Unsere Services sind modular aufgebaut und lassen sich individuell auf Ihre Anforderungen zuschneiden. So erhalten Sie genau die Sicherheitsmaßnahmen, die Ihr Unternehmen braucht.

Kontaktieren Sie uns: +49 5932 5009818 sales@alphasolid.de **alphasolid.de**

Analysieren

Security Vorab-Check

Analyse
Erfassung und **Auswertung** relevanter Daten zu:

- Backup-Strategien
- Active Directory
- Patch-Management
- Inventarisierung, Monitoring
- Firewall- und VLAN-Konfigurationen
- Endpoint-Sicherheit

Ergebnisse
Basierend auf den gewonnenen Erkenntnissen werden passende Sicherheitsmaßnahmen empfohlen. Detaillierte Besprechung der Empfehlungen, sofortige Implementierung kleinerer Verbesserungen während der Workshops und Dokumentation der durchgeführten Änderungen.

Penetrationstest

Vorsprung durch Sicherheit.
Finden und beheben Sie Schwachstellen, bevor Cyberangreifer sie ausnutzen können.

Penetrationstests sind unverzichtbarer Bestandteil jeder umfassenden IT-Sicherheitsstrategie. Unser Team aus professionellen IT-Security-Experten geht einen Schritt weiter: Wir hacken uns manuell in Ihre Systeme, um Schwachstellen viel gründlicher und effizienter zu identifizieren. Diese manuelle Vorgehensweise ermöglicht es uns, komplexe Sicherheitslücken aufzudecken, die automatisierte Tools oft übersehen.

Vorteile:

- **Identifikation und Behebung von Schwachstellen:**
  Ein Pentest deckt Sicherheitslücken in IT-Systemen, Anwendungen und Netzwerken auf, sodass diese proaktiv behoben werden können, bevor sie von böswilligen Angreifern ausgenutzt werden.
- **Verbesserung der Sicherheitsstrategie:**
  Die Ergebnisse liefern wertvolle Einblicke in die Effektivität Ihrer aktuellen Sicherheitsmaßnahmen und helfen dabei, gezielte Verbesserungen vorzunehmen.
- **Compliance und Risikominderung:**
  Ein Pentest unterstützt Sie dabei, Compliance-Anforderungen zu erfüllen und das Risiko von Datenverlusten, finanziellen Schäden und Reputationsverlusten zu minimieren.

Kontaktieren Sie uns: +49 5932 5009818 sales@alphasolid.de **alphasolid.de**

Red Teaming

Ihre Verteidigung gegen fortgeschrittene Bedrohungen

Red Teaming ist ein **spezialisierter Pentest-Service**, der über traditionelle Sicherheitsüberprüfungen hinausgeht. Es handelt sich um eine umfassende und realitätsnahe Simulation von Cyberangriffen, um die Verteidigungsstrategien und Sicherheitslücken Ihres Unternehmens zu testen. Dieser Service ist entscheidend für die Optimierung der IT-Sicherheit, da er Schwachstellen aufdeckt, bevor echte Angreifer diese ausnutzen können.

Vorteile:

- **Realistische Bedrohungssimulation:** Durch die Simulation realistischer Angriffe können Sie besser verstehen, wie Sie auf echte Bedrohungen reagieren würden. Szenarien werden aus der Sicht des Angreifers entwickelt.
- **Umfassende Sicherheitsbewertung:** Red Teaming deckt Schwachstellen in allen Bereichen auf, von der Netzwerkinfrastruktur bis hin zu physischen Sicherheitsmaßnahmen.
- **Verbesserte Sicherheitsstrategie:** Die Ergebnisse helfen Ihnen, Ihre Sicherheitsstrategien zu verfeinern und gezielte Maßnahmen zur Risikominimierung zu ergreifen.

Audits:
Passwort-Audit

Ihre digitalen Schlüssel im Härtetest

Was passiert bei unserem Passwort-Audit:

- Wir durchleuchten Ihr komplettes Active Directory
- Abgleich aller Passwörter mit über 1 Milliarde kompromittierter Kennwörter
- Identifikation von schwachen Passwörtern, Dubletten und ungeschützten Accounts
- Analyse von Admin-Konten und privilegierten Zugängen
- Überprüfung der Passwort-Richtlinien gegen Industriestandards (NIST, BSI, etc.)

Was Sie erhalten: Einen detaillierten Report mit Executive Summary – schwarz auf weiß dokumentiert, welche Accounts sofort geändert werden müssen und welche Richtlinien nachgeschärft gehören.

Warum das lebenswichtig ist: Ein einziges schwaches Admin-Passwort reicht aus, um dein gesamtes Netzwerk zu kompromittieren. Wir haben schon Unternehmen gesehen, bei denen 40% aller Passwörter bereits in Hacker-Datenbanken standen.

Management Risk Report

Ihre Angriffsfläche von außen

Unser External Risk Assessment umfasst:

- Scan Ihrer gesamten externen IT-Infrastruktur – genau wie ein Hacker es tun würde
- Identifikation offener Ports und ungeschützter Services
- Analyse veralteter Software und bekannter Vulnerabilities
- SSL/TLS-Schwachstellen und Zertifikatsprobleme
- DNS-Sicherheit und E-Mail-Konfiguration
- Web-Anwendungs-Security und Server-Härtung

Was Sie bekommen: Einen Management-Report mit priorisierten Handlungsempfehlungen, Risikobewertung und Budget-Planung für die Geschäftsführung.

Der Clou: Sie siehen Ihr Unternehmen durch die Augen eines Angreifers – bevor er zuschlägt. Keine Überraschungen mehr bei Penetrationstests oder Audits.

ITQ Basisaudit

Analyse:
Die ITQ-Basisprüfung kontrolliert die organisatorischen und technischen Schutzmaßnahmen in Ihrem Unternehmen, die für ein angemessenes Informationssicherheitsniveau erforderlich sind. Im Rahmen eines tiefergehenden Interviews mit den verantwortlichen Personen, das sich am BSI-Grundschutz ausrichtet, wird das Ergebnis ermittelt.

Ergebnisse:
Die einzelnen Maßnahmenempfehlungen werden priorisiert und gleich Verantwortlichkeiten festgelegt, so dass ein konkreter Projektplan für die Umsetzung in Ihrem Unternehmen entsteht. Sie werden fortan eine ausgereifte Grundlage zur Planung des IT-Budgets vorliegen haben und können anhand dieser Grundlage entsprechende Aufgaben, auch ohne notwendiges Fachwissen, delegieren.

Phishing-Test

Vor Phishing-Angriffen sicher.

Testen und stärken Sie die Reaktionsfähigkeit Ihrer Mitarbeitenden gegen Cyberbedrohungen.

Ein Phishing Test ist eine gezielte Sicherheitsüberprüfung, bei der simulierte Phishing Mails an Ihre Mitarbeiter gesendet werden. Ziel ist es, die Reaktionen der Mitarbeiter auf solche E-Mails zu testen und zu sehen, wie viele und welche Art von E-Mails sie öffnen, auf Links klicken oder sensible Daten preisgeben. Diese Tests helfen dabei, Schwachstellen in der Schulung und Sensibilisierung der Mitarbeiter zu identifizieren und gezielte Maßnahmen zur Verbesserung Ihrer IT-Sicherheit zu ergreifen.

Erhöhen Sie Ihre Sicherheit: Die 3 größten Vorteile eines effektiven Phishing-Tests

Sicherheitsbewusstsein der Mitarbeiter erhöhen
Durch regelmäßige Phishing Tests wird das Sicherheitsbewusstsein der Mitarbeiter geschärft, sodass sie potenzielle Bedrohungen schneller erkennen und besser darauf reagieren können, was das Risiko von Sicherheitsvorfällen reduziert.

Schwachstellen in der Sicherheitsstrategie aufdecken
Phishing Tests helfen dabei, Schwachstellen in der aktuellen Sicherheitsstrategie zu identifizieren. Sie zeigen auf, wo zusätzliche Schulungen oder technische Maßnahmen notwendig sind, um die Abwehrkräfte zu stärken.

Allgemeine Sicherheitskultur stärken
Regelmäßige Phishing Tests fördern eine Kultur der Wachsamkeit und des sicheren Umgangs mit E-Mails, wodurch das gesamte Unternehmen sicherer wird und Mitarbeiter proaktiv Ihr Unternehmen vor Bedrohungen schützen.

Web Application Pentest

Webanwendungen sind oft das Einfallstor für Angreifer – SQL-Injection, Cross-Site-Scripting oder unsichere APIs können kritische Geschäftsprozesse gefährden. Unser Web Application Pentest kombiniert automatisierte Scans mit manueller Expertise, um auch komplexe Schwachstellen aufzudecken.

Vorteile:
Die Kombination aus automatisierter Abdeckung und menschlicher Expertise deckt Schwachstellen auf, die reine Scanner übersehen. Tests erfolgen realitätsnah aus Angreiferperspektive – inklusive Chaining mehrerer Schwachstellen zu kritischen Angriffspfaden.

Ergebnis:
Vollständiges Verständnis der Sicherheitslage deiner Webanwendungen, priorisierte Schwachstellen mit Ausnutzungsszenarien und klare Handlungsempfehlungen für Entwickler und Security-Teams.

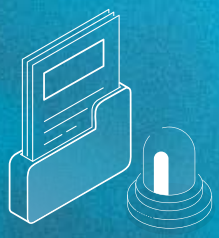
Forensic

Nach einem Sicherheitsvorfall zählt jede Minute. IT-Forensik sichert Beweise, rekonstruiert Angriffswege und liefert die Grundlage für rechtliche Schritte, Versicherungsfälle und nachhaltige Härtungsmaßnahmen.

Vorgehensweise:
Alle Maßnahmen erfolgen nach forensischen Standards, um Beweismittel gerichtsfest zu sichern. Die Analyse läuft parallel zur Wiederherstellung – ohne den laufenden Betrieb unnötig zu verzögern.

Ergebnis:
Lückenlose Aufklärung des Vorfalls, rechtssichere Dokumentation und konkrete Maßnahmen, um ähnliche Angriffe künftig zu verhindern. Du weißt nicht nur, dass etwas passiert ist – sondern wie, warum und was jetzt zu tun ist.

Schützen



AD-Härtung

Absichern und Aufräumen

In insg. 5 Workshops gehen wir die grundlegenden Themen an:

- AD organisieren und Aufräumen (2 Workshops)
- Verschlüsselte Kommunikation
- Authentifizierung & Crypt = Up2Date
- Round Up & Offene Themen

Backup-Härtung

Schreib- und Löschschutz

Das gehärtete Repository bietet einen Schreib- und Löschschutz für Backupdateien. Die Dateien werden mit einer Art „Zeitschloss“ versehen und können selbst mit root-Rechten nicht mehr gelöscht werden.

Umsetzung

- Presales: Sizing Backup & Storage-Bedarf
- Inbetriebnahme des Linux- und Windows-Servers.
- Konfiguration des Immutable Repositories
- Installation & Konfiguration der Veeam Infrastruktur
- Erstellen der Backup-Jobs
- Nacharbeiten / Anpassen der Jobs / Übergabe

Admin-Tiering

Segmentierung des AD

Das Konzept lebt davon, keine allgemeingültigen Administrationskonten zu verwenden. Wer unseren Empfehlungen folgt (Priviliged Access Workstations, Passwort-Manager, RDP-Manager, etc.) verursacht keinen administrativen Mehraufwand.

Die Umsetzung erfolgt im Workshop-Format.

Das Projekt wird in 5 Phasen (Workshops) unterteilt:

Phase 0: Heranführung: Erklärung, Begutachtung, Prüfen der AD
Phase 1: Integration: Tiers/Klassen definieren, Anpassung des AD
Phase 2: Migration: Systeme werden überführt, neue Konten genutzt
Phase 3: Bereinigung: Alte Admin-Accounts werden entfernt
Phase 4: Härtung: Definition sicherer Standards und automatische Aktivierung/Deaktivierung

Desaster Restore Tests

Notfallwiederherstellung

Wiederherstellung des Repositorys auf auf einer separaten Hardware (von Alphasolid zur Verfügung gestellt), um zu überprüfen,

- ob alle relevanten Informationen für den Zugriff auf das Backup vorhanden sind.
- ob der Inhalt des Backups für einen Wiederanlauf genutzt werden kann.
- welches Zeitfenster für die Wiederherstellung benötigt wird.

Umsetzung
Temporärer Aufbau der Hardware im Rechenzentrum des Kunden

- Installation der Hypervisor Instanzen
- Einbindung in die Infrastruktur
- Restore der Daten
- Testen der wiederhergestellten VMs
- Berichtserstellung mit Zusammenfassung der Ergebnisse

Incident Response

Sofortige Unterstützung nach einem IT-Sicherheitsvorfall

Verlieren Sie keine Zeit! Wir bieten sofortige und wirkungsvolle Hilfe bei Cyberangriffen auf Ihr Unternehmen.

Warum nach einem Cyberangriff schnelles Handeln entscheidend ist
Nach einem Cyberangriff ist sofortiges Handeln entscheidend, um den Schaden zu minimieren und die Sicherheit Ihrer IT-Infrastruktur wiederherzustellen. Jede Verzögerung kann zu weiterem Datenverlust, finanziellen Schäden und Reputationsverlust führen. Durch eine umgehende Reaktion können Schwachstellen identifiziert, die Ursachen des Vorfalls analysiert und Maßnahmen zur Wiederherstellung Ihrer Systeme ergriffen werden. Unsere Experten stehen an Ihrer Seite, um schnell und effektiv auf den Sicherheitsvorfall zu reagieren und Ihre Systeme zu sichern.

Wir leiten alle notwendigen Maßnahmen ein, um Ihre Daten zu schützen.

Schnelle & Effektive Krisenbewältigung:

Sofortige Reaktion auf Vorfälle
Unser erfahrenes Team für IT-Security ist darauf trainiert, blitzschnell zu reagieren und die Situation unter Kontrolle zu bringen.

Detaillierte Vorfallsberichte
Nach jedem Vorfall erhalten Sie umfassende Berichte und Analysen, um die Ursachen zu verstehen und zukünftige Risiken zu minimieren.

Wiederherstellungs- und Präventionsstrategien
Wir stellen Ihre Systeme wieder her und entwickeln präventive Maßnahmen zum zukünftigen Schutz Ihrer Daten.

Sensibilisieren

Awareness Trainings

Schulungen und Awareness-Programme für eine sichere IT-Umgebung

Ein wesentlicher Bestandteil der IT-Sicherheit ist das Bewusstsein und die Kompetenz Ihrer Mitarbeiter im Umgang mit potenziellen Bedrohungen. Unsere Schulungen und Awareness-Programme sind darauf ausgerichtet, Ihre Belegschaft für die Risiken der digitalen Welt zu sensibilisieren und ihnen das nötige Wissen zu vermitteln, um sicher und verantwortungsvoll mit IT-Ressourcen umzugehen. Durch praxisnahe Workshops und maßgeschneiderte Trainingsmodule erhöhen wir das Sicherheitsbewusstsein in Ihrem Unternehmen.

Security Awareness Training

Sensibilisieren Sie Ihre Mitarbeiter vor Phishing Mails

Security Awareness Trainings sind ein essenzieller Bestandteil jeder umfassenden IT-Sicherheitsstrategie. Bei alphasolid bieten wir nicht nur grundlegende Schulungen an, sondern gehen einen Schritt weiter, um sicherzustellen, dass Ihre Mitarbeiter bestens auf Cyberbedrohungen vorbereitet sind. So stellen wir sicher, dass Ihr Unternehmen optimal gegen Cyberangriffe geschützt ist und eine starke Sicherheitskultur entwickelt.

Sicherer durch Wissen: Die größten Vorteile unseres Trainings

Erhöhtes Sicherheitsbewusstsein und Prävention
Unser Security Awareness Training sensibilisiert Ihre Mitarbeiter für die neuesten Cyberbedrohungen und schult sie darin, verdächtige Aktivitäten und Phishing-Versuche zu erkennen. Gut geschulte Mitarbeiter sind weniger anfällig für Angriffe, was das Gesamtsicherheitsniveau Ihres Unternehmens erheblich verbessert.

Reduzierung von Sicherheitsvorfällen
Durch die Schulung Ihrer Mitarbeiter in Best Practices der IT-Sicherheit und der Erkennung von Bedrohungen kann die Häufigkeit und Schwere von Sicherheitsvorfällen deutlich reduziert werden. Dies führt zu weniger Unterbrechungen im Geschäftsbetrieb und schützt Ihre wertvollen Daten.

Compliance und Risikominderung
Viele Branchenvorschriften erfordern regelmäßige Sicherheits- und Awareness-Schulungen für Mitarbeiter. Unser Training unterstützt Ihr Unternehmen dabei, diese Compliance-Anforderungen zu erfüllen und das Risiko von Datenschutzverletzungen, finanziellen Verlusten und Reputationsschäden zu minimieren.

Managed Services

Alphasolid Honeypot

Angreifer im Netz? Sie erfahren es sofort.

Die meisten Unternehmen merken viel zu spät, dass sie gehackt wurden. Der Alphasolid Honeypot ändert das Spiel: Digitale Frühwarnsysteme geben Ihnen Bescheid, sobald jemand dort schnüffelt, wo er nicht hingehört.

Das Prinzip: Täuschung als Frühwarnsystem

Angreifer, die in ein Netzwerk eindringen, suchen nach wertvollen Zielen. Sie durchforsten Fileserver, testen Zugangsdaten und scannen nach verwundbaren Systemen. Genau hier setzen Hardware Honeypots und Canary Tokens an: Sie sehen aus wie echte Systeme und Assets – sind aber präparierte Köder, die bei Berührung sofort eine Warnung auslösen.

Hardware Honeypots

Täuschend echte Systeme:

- Physische Geräte, die gezielt als Täuschungsziele in Ihr Netzwerk integriert werden
- Simulieren echte Netzwerkgeräte wie Windows-Server, Router oder Linux-Systeme
- Emulieren verschiedene Dienste: Windows-Dateifreigaben, SSH-Server, Webserver, Datenbanken, Netzwerk-Router und mehr

Vorteile:

- **Praktisch keine Fehlalarme:** Legitime Nutzer haben keinen Grund, mit einem Honeypot zu interagieren
- **Verschlüsselte Kommunikation:** Alle Daten werden sicher übertragen
- **Täuschend realistisch:** Die Emulation ist so präzise, dass Angreifer ein echtes System vor sich wähnen
- **Honeypot-Scanner-Erkennung:** Erkennt Tools, die gezielt nach Honeypots suchen

Canary Tokens

Digitale Fallen für jeden Einsatzort:

- Gefälschte digitale Assets, die überall platziert werden können
- Dokumente, die beim Öffnen alarmieren
- Fake-Zugangsdaten (AWS-Keys, API-Tokens, Passwörter)
- URLs und DNS-Namen, die jeden Zugriff tracken
- QR-Codes für physische Sicherheit

Die Kombination macht den Unterschied:
Hardware Honeypots sichern Ihr Netzwerk auf Geräteebene ab, Canary Tokens erweitern diesen Schutz auf die Datenebene. Zusammen bilden sie ein dichtes Frühwarnnetz, das Eindringlinge auf jedem Level erkennt.

SOC Response Check

Ihre IT steht unter Beschuss – aber reagiert Ihr SOC auch?

Weil ein SOC unter Realbedingungen ganz anders reagiert als in der Theorie. Als unabhängiger Dritter testen wir Ihr SOC mit den aktuellen Taktiken, Techniken und Prozeduren (TTPs) echter Cyberakteure.

Was wir testen:

- **Angriffssimulation:** Initial Access, Lateral Movement, Datenexfiltration – alles, was Angreifer heute drauf haben
- **Reaktionsgeschwindigkeit:** MTTD und MTTR unter Realbedingungen – keine Theorie
- **Alarmierung:** Funktionieren Ihre Eskalationsprozesse wirklich?
- **Detection-Qualität:** Erkennt Ihr SOC, was es erkennen muss?

Was Sie davon haben:

- **Transparenz:** Schwarz auf weiß, wie gut Ihr SOC wirklich ist
- **Klarheit:** Stärken, Schwächen, konkrete Verbesserungsvorschläge
- **Sicherheit:** Quartalsweise Kontrolle für kontinuierlichen Schutz
- **Objektivität:** Neutrale Bewertung durch externe Experten

Das Ergebnis:
Mit dem SOC Response Check erhalten Sie einen kompakten Report mit klarer Beurteilung und konkreten Handlungsempfehlungen. Damit wissen Sie: Ihr SOC schützt nicht nur theoretisch – es schützt tatsächlich.

External Attack Surface Management (EASM)

Die Angriffsfläche Ihres Unternehmens wächst kontinuierlich – durch Cloud-Services, Schatten-IT, Fusionen oder vergessene Subdomains. Mit unserer EASM-Plattform verschaffen Sie sich einen Überblick über alle extern erreichbaren Assets und identifizieren Schwachstellen, bevor Angreifer sie ausnutzen.

Vorteile:
Ein EASM arbeitet aus Angreiferperspektive: Was kann ein Hacker sehen? Wo sind die Einfallstore? Die Plattform deckt blinde Flecken auf, die traditionelle Vulnerability-Scanner übersehen – von vergessenen Entwicklungsservern bis zu exponierten S3-Buckets.

Ergebnis:
Vollständige Transparenz über Ihre externe Angriffsfläche, priorisierte Maßnahmen zur Risikominimierung und kontinuierliche Überwachung neu hinzukommender Assets.

Credential Monitoring

Kompromittierte Zugangsdaten sind der Haupteinstiegsvektor für Cyberangriffe. Mit dem Credential Monitoring wird kontinuierlich überwacht, ob Credentials Ihrer Organisation im Dark Web, in Paste-Sites oder Leak-Datenbanken auftauchen – bevor Angreifer sie missbrauchen.

Ergebnis:
Frühwarnsystem für kompromittierte Zugangsdaten. Sie erfahren von geleakten Credentials, bevor sie für Credential Stuffing, Phishing oder gezielte Angriffe genutzt werden.

Dark Web Monitoring

Das Dark Web ist Umschlagplatz für gestohlene Daten, Angriffspläne und Insider-Informationen. Unser Dark Web Monitoring durchsucht versteckte Foren, Marktplätze und Telegram-Kanäle nach Erwähnungen Ihres Unternehmens, geleakten Informationen oder geplanten Angriffen.

Ergebnis:
Threat Intelligence aus erster Hand. Sie wissen, was im Untergrund über Ihr Unternehmen kursiert und können proaktiv reagieren, bevor aus Informationen Angriffe werden.

Specops Password Policy

Maximale Passwort-Sicherheit für Ihr Active Directory

Specops Password Policy erweitert Ihre bestehenden Active Directory-Gruppenrichtlinien um professionelle Passwort-Sicherheit. Blockieren Sie kompromittierte Passwörter automatisch und reduzieren Sie Cyberrisiken – ohne Zusatzserver oder komplexe Installation.

Top Features:

- **Schutz vor 4+ Milliarden kompromittierter Passwörter:** Blockiert täglich aktualisierte Passwörter aus Datenlecks und Live-Angriffen
- **Erweiterte Richtlinien:** Unbegrenzte Wörterbücher, 5 Zeichentypen, Passphrase-Support
- **Automatische Überwachung:** Tägliche Scans mit sofortiger Benachrichtigung bei Risiken
- **Benutzerfreundlich:** Echtzeit-Feedback und anpassbare Meldungen

Die 3 wichtigsten Vorteile:
1. Maximale Sicherheit: Automatischer Schutz vor neuesten Cyberbedrohungen durch die weltweit größte Datenbank kompromittierter Passwörter
2. Weniger Helpdesk-Aufwand: Klare Passwort-Anforderungen und Echtzeit-Feedback reduzieren Benutzeranfragen drastisch
3. Einfache Integration: Nahtlose Einbindung in bestehende Active Directory-Umgebungen ohne zusätzliche Server