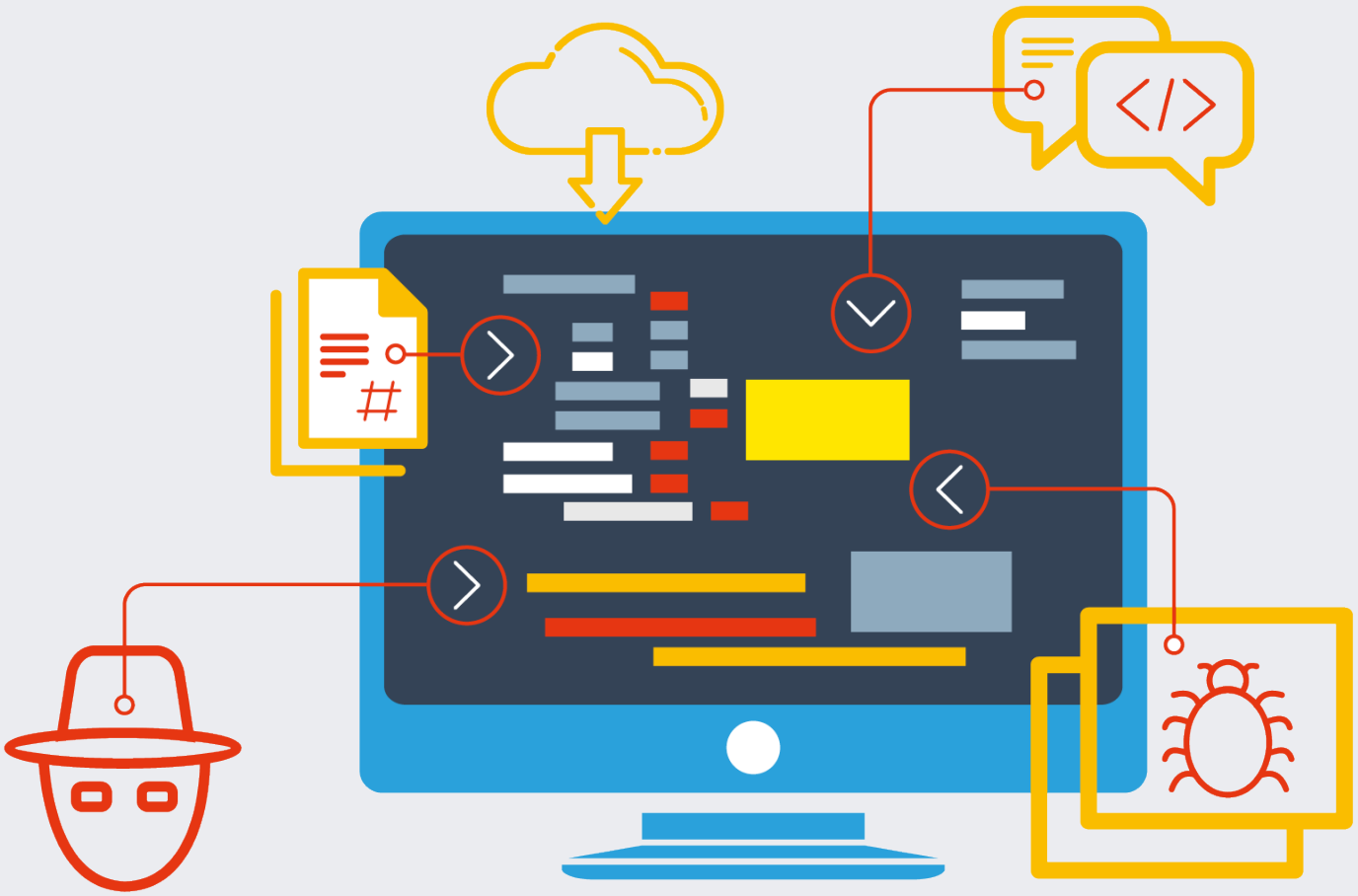
Outpost24

Sicherheit erhöhen, Kosten sparen

Pentesting as a Service für Webapplikationen



Sicherheit erhöhen, Kosten sparen

Pentesting as a Service für Webapplikationen

Bei Cyberangriffen spricht alle Welt von Ransomware. Die Gefahr ist zwar nicht zu unterschätzen, muss aber relativiert werden. Studien zeigen, dass 56 Prozent[1] der hundert größten Sicherheitsvorfälle in den vergangenen fünf Jahren auf Sicherheitsprobleme bei Webanwendungen zurückgingen. Im Schnitt weist jede Website 15 Schwachstellen[2] auf, von denen zwei schwerwiegend sind, außerdem haben es die Angreifer nicht nur auf Kommunikations[3]- und Kundendaten abgesehen. Immer öfter geraten auch Zugangsdaten für Cloud-Dienste und kritische Business-Informationen wie zum Beispiel Marktanalysen oder die Preisgestaltung ins Visier von Kriminellen.

Ist eine Schwachstelle in einer Webapplikation erst einmal ausspioniert oder bekannt geworden, dauert es in der Regel nur wenige Tage bis zur Attacke. Die Frage ist also nicht mehr ob, sondern wann der Angriff erfolgt. Eine Studie von Outpost24[4] hat exemplarisch die Chemiebranche analysiert. Sie zeigt, dass 60 Prozent der Hersteller „kritisch gefährdet" sind. Die Bandbreite der Anfälligkeiten reicht von veralteten Komponenten bis hin zu kompromittierten Anmeldeinformationen von Benutzern. Die Bedrohung im Cyberraum sei so hoch wie noch nie, mahnt das Bundesamt für Sicherheit in der Informationstechnik (BSI)[5] in seinem Report zur Lage der IT-Sicherheit in Deutschland 2022. Demnach bedrohen unter anderem DDoS-Angriffe die Informationssicherheit insbesondere von Online-Shops und Anbietern webbasierter Dienste.

Sie müssen dringend Abwehrmaßnahmen ergreifen. Noch besser ist es allerdings, den Angreifern zuvorzukommen, indem man Lücken, fehlerhafte Programmierungen, Logikfehler oder falsche Konfigurationen selbst aufdeckt und sie ausmerzt, bevor sie andere entdecken.

[1] **F5:** The State of the State of Application Exploits in Security Incidents (https://www.f5.com/content/dam/f5-labs-v2/article/pdfs/The-State-of-the-State-of-Application-Exploits-in-Security-Incident-F5Labs-rev22JUL21.pdf).

[2] **Positive Technologies:** Threats and vulnerabilities in web applications 2020–2021 (https://www.ptsecurity.com/ww-en/analytics/web-vulnerabilities-2020-2021/#:~:text=The%20most%20dangerous%20vulnerabilities%20in,vulnerabilities%20in%20the%20oAuth%20protocol).

[3] **Bitkom:** Wirtschaftsschutz 2022 (https://www.bitkom.org/sites/main/files/2022-08/Bitkom-Charts_Wirtschaftsschutz_Cybercrime_31.08.2022.pdf).

[4] **Outpost24:** 2022 Web Application Security for Chemical Manufacturing Report (https://outpost24.com/resources/whitepapers/2022-web-application-security-for-chemical-manufacturing-report).

[5] **BSI:** Die Lage der IT-Sicherheit in Deutschland 2022 (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=6).

Klassisches Penetration Testing gilt als probates und oft genutztes Mittel für diesen Zweck: Dabei werden die eigenen Applikationen und Systeme mittels eines autorisierten und simulierten Angriffs auf den Prüfstand gestellt. Die Pentester verhalten sich dabei möglichst so, wie mutmaßlich auch Cyberkriminelle vorgehen würden. Das stellt reale Bedingungen des Tests sicher, hat aber auch Nachteile: Zum einen ist der Aufwand hoch, zum anderen dauert es sehr lange, bis der Test definiert und durchgeführt ist, die Schwachstellen identifiziert, analysiert und gestopft sind. Hinzu kommt, dass es sich dabei nur um Momentaufnahmen handelt. Es treten nur die Schwachstellen hervor, die zum Zeitpunkt des Tests bestehen. Nach einem Software-Update oder dem Ausrollen einer neuen Version einer Applikation kann die Situation schon wieder ganz anders aussehen. Mit Pentesting as a Service (PtaaS) kommen Firmen vor die Angriffswelle.

Was klassische Pentests können

Daten zählen mittlerweile zum wichtigsten Gut von Unternehmen oder Behörden. Ob es sich um ein Kundenportal, einen Webshop, das Intranet oder Online-Banking handelt: Die Sicherheit der Informationen steht an erster Stelle. Es existieren bereits zahlreiche gesetzliche Vorschriften, die diesbezüglich einzuhalten sind. Das gilt besonders für Unternehmen und Einrichtungen der Kritischen Infrastruktur, etwa Energieversorger. Das Schutzniveau sollte aus eigenem Interesse so hoch wie möglich gehalten werden, weil zu viel auf dem Spiel steht. Die Zeiten, in denen Cyberkriminelle „nur“ ein paar Daten abgreifen wollten, sind längst vorbei. Die Kompromittierung von Kunden- oder Bezahlinformationen ist zwar nach wie vor ein Ziel vieler Angreifer. Es gibt mittlerweile aber auch viele andere kriminelle Geschäftsmodelle wie etwa das Kapern oder gar das Zerstören ganzer Webplattformen. Die Folgen reichen von Umsatz- und Imageverlust bis hin zur Insolvenzgefahr.

Pentests funktionieren diesbezüglich sehr gut, weil sie eine sehr praxisnahe Form der Schwachstellenidentifikation verfolgen. Sicherheitsexperten besprechen gemeinsam mit dem Kunden das Set-up des Tests. Dabei wird unter anderem festgelegt, welche Bereiche wie getestet werden sollen. In der Praxis haben sich drei verschiedene Herangehensweisen als Best Practices herauskristallisiert.

Arten von Penetration Tests

- Bei einem **Black-Box-Test** verfügt der Pentester über keinerlei Hintergrundinformationen. Er sucht allein auf Basis seiner Fertigkeiten und seines Wissens nach Schwachstellen in der Webapplikation. Solche Tests benötigen zwar am wenigsten Vorbereitungszeit, doch der Pentester arbeitet unter Zeitdruck. Im realen Leben haben Hacker praktisch unendlich viel Zeit, um so lange zu suchen, bis sie eine Lücke finden. Die Aussagekraft von Black-Box-Tests bleibt somit begrenzt.

- Bei einem **Gray-Box-Test** erhält der Pentester einige Hintergrundinformationen. Er wird außerdem als Nutzer des Systems authentifiziert, startet also nicht bei null.

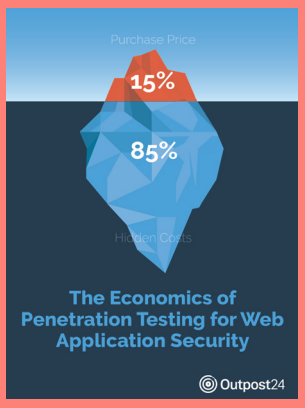
- Bei einem **White-Box-Test** wird der Tester im Vorfeld nicht nur mit ausführlichen Hintergrundinformationen versorgt, er erhält auch Admin- beziehungsweise Zugriffsrechte auf Root-Ebene. Damit erzielen solche Tests zwar die aussagekräftigsten Ergebnisse, sie benötigen aber auch viel Vorbereitung und kosten entsprechend viel Geld.

Klassische Pentests gewährleisten also bereits einen fortgeschrittenen individuellen Ansatz und helfen dabei, die Sicherheit der eigenen Webapps zu optimieren. Darüber hinaus können sie, richtig aufgesetzt, auch als Nachweis von Compliance-Pflichten dienen – und somit zwei Fliegen mit einer Klappe schlagen. Wer seine Webapplikationen mittels eines Pentests auf Herz und Nieren prüfen lässt, genießt außerdem das gute Gefühl, grundsätzlich gewappnet zu sein gegen Angriffe und daraus resultierende negative Folgen.

Was klassische Pentests nicht können

„Grundsätzlich“ bedeutet in diesem Zusammenhang, dass klassische Pentests leider auch einige gravierende Schwachstellen aufweisen. Jede Medaille hat zwei Seiten: Das individuelle Aufsetzen des Tests geht mit viel Aufwand einher – und das kostet Zeit. Am Anfang steht die Abstimmung miteinander, dann folgt das Festlegen von Umfang und Zielen. Nach dem Angebot, der Auftragserteilung und der Durchführung fängt die Arbeit erst richtig an: Die Ergebnisse müssen präzise gedeutet, richtig priorisiert und in konkrete Maßnahmen umgemünzt werden. Angesichts ellenlanger Dokumentationen, die manche Anbieter ihren Kunden liefern, fällt das auch IT-Fachleuten oftmals schwer – für IT-Admins in Unternehmen ohne eigenes Security Department ist es nahezu unmöglich. Hinzu kommt, dass die Überprüfung der Behebung von gefundenen Schwachstellen in der Regel nicht zu den Bestandteilen klassischer Pentests für Webanwendungen zählt. Dafür müssen andere Tools her, die ebenfalls Geld kosten und Know-how erfordern. Die Folge: Bis die Fehler behoben sind, vergeht viel zu viel Zeit.

Das gilt insbesondere angesichts immer kürzer werdender Release-Zyklen. Die mangelnde Flexibilität macht es schwer bis unmöglich, auf wechselnde Bedarfe einzugehen. Klassische Pentests berücksichtigen keine Veränderungen: Wie ein Screenshot wird lediglich der Status quo zu einem festgelegten Zeitpunkt analysiert. Was passiert aber, wenn sich die Webapplikation grundlegend geändert hat, Anwendungen neu eingeführt oder alte offline genommen wurden? Den gesamten Prozess von vorne zu beginnen, ist zwar eine Alternative, aber eine teure und keine gute.

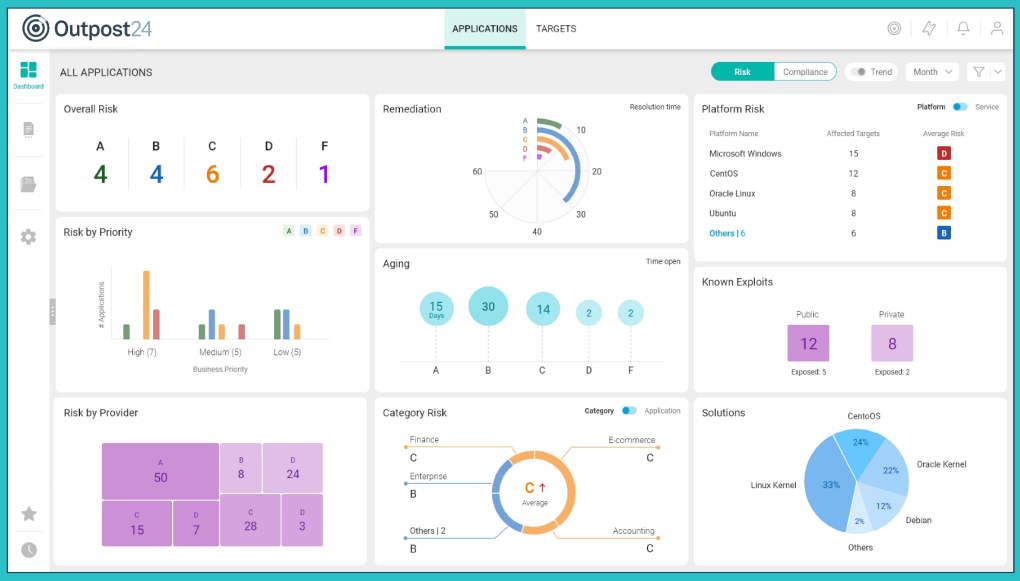


Apropos Kosten:
Oftmals umfassen Angebote für klassische Pentests kaum mehr als den Test selbst. Zu dem Fixbetrag kommen in der Praxis aber noch viele interne Kosten hinzu, etwa für die Vor- und Nachbereitung, für die Analyse und für die konkrete Fehlerfindung. Diese versteckten Kosten können sich auf ein Vielfaches der ursprünglich eingeplanten Kosten summieren. Lesen Sie mehr dazu in diesem **Outpost24-Whitepaper**.

Was Pentesting as a Service (PtaaS) auszeichnet

Pentesting as a Service von Outpost24 bietet die Vorteile klassischer Pentests, aber ohne die Nachteile. Im Vergleich treten keinerlei Abstriche in punc-to Umfang oder Qualität auf. Im Gegenteil: Der Schutz ist umfassender und gleichzeitig flexibler. Im Einzelnen funktioniert das so:

- PtaaS verbindet automatische Sicherheitsscans mit manuellen Tests. Das deckt viele verschiedene Gefahren auf. Geprüft werden nicht nur die Webapplikationen selbst, sondern je nach Scope auch Testumgebungen und von den Anwendungen verwendete Schnittstellen. Laufzeit-Schwachstellen treten ebenso hervor wie Fehler in der dahinterliegenden Business-Logik. Die Anzahl potenzieller Schwachstellen ist größer, als viele Menschen denken. Sie reicht von einer fehlerhaft konfigurierten Zugriffskontrolle auf sensible Daten über veraltete kryptografische Algorithmen und Protokolle bis hin zu Injection-Attacken, bei denen eine Webanwendung zum Ausführen von schädlichen Codes gezwungen werden kann.

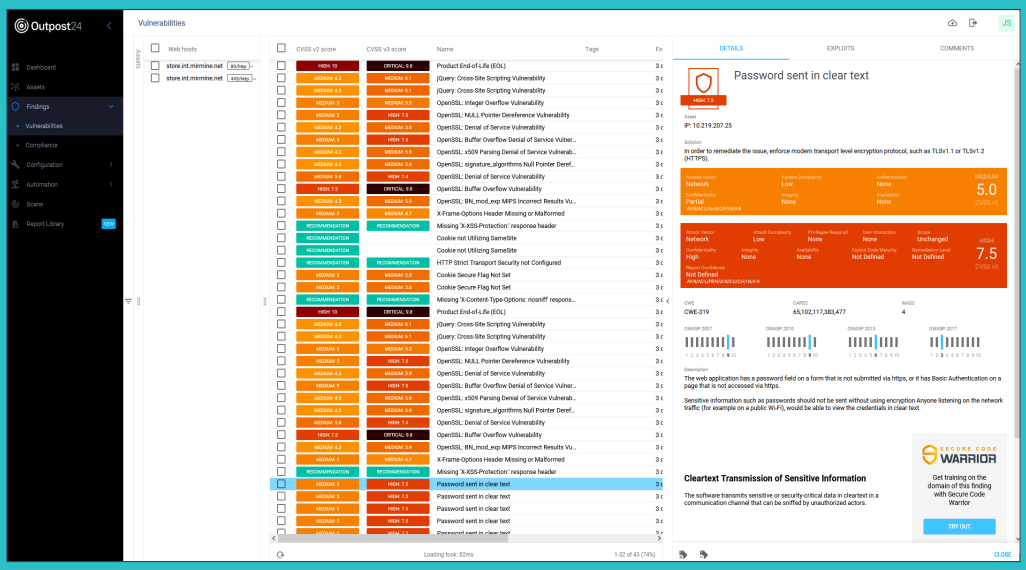


Übersichtliches Reporting bereits während des Pentests beschleunigt die Umsetzung von Gegenmaßnahmen.

- Zertifizierte Sicherheitsexperten von Outpost24 prüfen, verifizieren und priorisieren die Ergebnisse der Tests. Das stellt sicher, dass sich Kunden mit keinerlei Falschmeldungen herumschlagen müssen, die am Ende nur Zeit und Geld kosten.

- Stattdessen erhalten sie nur relevante Meldungen und sehen aufgrund der risikobasierten Priorisierung auf einen Blick, wo dringender oder weniger dringender Handlungsbedarf besteht. Die Bewertung erfolgt dabei nicht nur auf Basis klassischer Risikokategorisierungen, es fließen auch qualifizierte Erkenntnisse der Outpost24-eigenen Threat-Intelligence-Analysen ein. Das führt insgesamt zu noch individuelleren und hochwertigeren Ergebnissen.

- Kunden können gefundene Schwachstellen und empfohlene Fixes in Echtzeit über ein zentrales Dashboard abrufen. Das reduziert die Reaktionszeit im Vergleich zu klassischen Pentests erheblich. Sie müssen nicht mehr auf ein kryptisches und seitenlanges Dokument nach Abschluss aller Tests warten, sondern können sich sofort über die erkannten und von Sicherheitsexperten verifizierten Schwachstellen informieren. Brauchen sie dabei Unterstützung, können sie jederzeit über die Plattform Kontakt mit einem Pentester aus dem Red Team von Outpost24 aufnehmen.

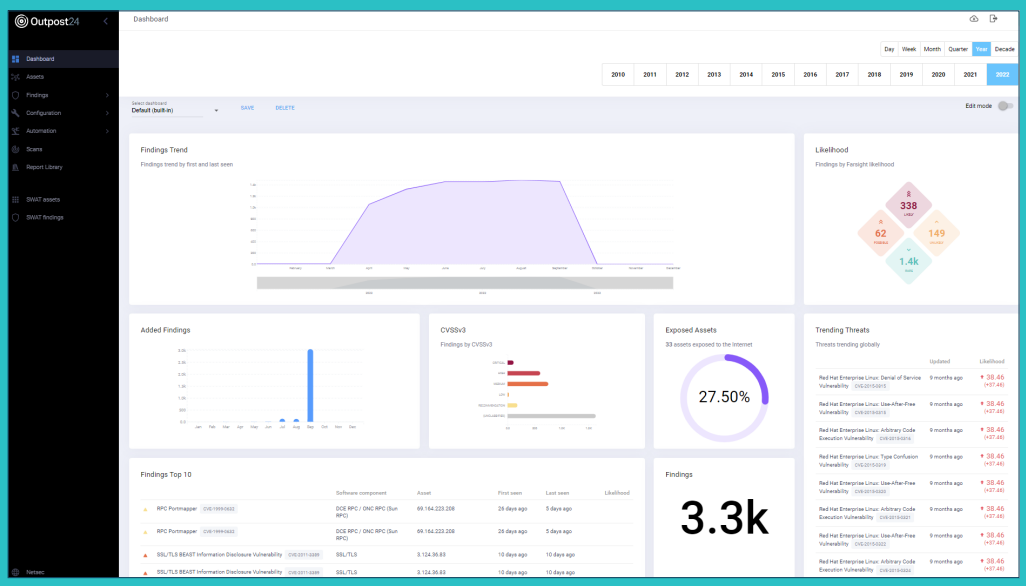


Detailliertes Reporting jeder einzelnen Schwachstelle erspart wertvolle Recherchezeit. Bei Rückfragen kann direkt ein Dialog zum Pentester geöffnet werden.

- Es erfolgt eine Prüfung der Korrekturen. Das stellt sicher, dass eine Gefahr nicht nur erkannt, sondern auch definitiv gebannt wurde.

- Veränderungen fließen durch kontinuierliches Monitoring ein. Dazu zählen zum einen regelmäßig wiederholte automatische Scans. Sie spielen vor allem vor dem Hintergrund schneller Release-Zyklen eine wichtige Rolle. Zum anderen decken manuelle Pentests Exploits auf, die automatische Pentests

nicht erkennen können. Kommen beim kontinuierlichen Monitoring neue Schwachstellen ans Licht, wird auch ihr Ausmaß schnell verifiziert und der Kunde informiert.



Eine risikobasierte Bewertung stellt sicher, dass Sie die kritischsten Schwachstellen entsprechend priorisieren könnnen.

All das führt zu einem flexiblen Schutzmantel mit großer Zeitersparnis und damit schnellerer Fehlerbehebung. Die von den Sicherheitsexperten konkret empfohlenen Maßnahmen lassen sich umgehend umsetzen. Auch business-seitig glänzt das PtaaS-Modell mit Pluspunkten: Der Verwaltungsaufwand und die Kosten für Pentests sinken. Gleichzeitig steigt die Flexibilität und Effizienz der IT-Security-Teams, da diese weniger damit beschäftigt sind, sich durch Schwachstellenanalysen und mehrseitige PDF-Reports wühlen müssen. Den Umfang von PTaaS können Kunden weiterhin ganz beliebig festlegen.

VERÄNDERUNGEN FLIESSEN DURCH KONTINUIERLICHES MONITORING EIN.

Wie sicher Pentesting as a Service ist

Es liegt in der Natur der Sache, dass Pentests Vertrauen zum Dienstleister voraussetzen, schließlich wird ihm nicht nur Zugriff auf sensible Daten und Applikationen gewährt. Viel stärker fällt ins Gewicht, dass seine Aufgabe darin besteht, Schwachstellen und Fehler zu finden. Geraten diese Informationen in falsche Hände, sind Cyberkriminellen Tür und Tor geöffnet. Deshalb sollte die Auswahl des ausführenden Unternehmens nicht auf die leichte Schulter genommen und erst recht nicht allein anhand des günstigsten Angebots getroffen werden.

Zu den wichtigsten vertrauensbildenden Maßnahmen zählen anerkannte Zertifizierungen. Sie belegen, dass die angebotenen Produkte und Dienstleistungen höchsten Standards sowie den Best Practices einer Branche entsprechen.

Im Bereich Pentesting zählen dazu beispielsweise

- **ISO 27001.** Dabei handelt es sich um eine international anerkannte Norm für Informationssicherheits-Management-Systeme. Sie legt unter anderem fest, welche Bedingungen ein solches System erfüllen muss, um die Informationssicherheit einer Firma, Behörde oder Institution zu überwachen und zu verbessern.

- **CREST.** Das ist eine international anerkannte und gemeinnützige Organisation, die die weltweite Cybersecurity-Industrie repräsentiert. Ein Schwerpunkt liegt auf Pentests, zu denen sie zahlreiche Schulungen anbietet. Wer eine Zertifizierung erhält, zählt zu einem derzeit rund 300 Mitglieder umspannenden Netzwerk von Sicherheitsexperten.

- **Certified Ethical Hacker.** Jeder kann lernen, Hacker zu werden. Zertifizierte Ethical Hacker haben ein professionelles Verständnis für IT, Netzwerke und Programmierung. Im Gegensatz zu den Hackern auf der dunklen Seite der Macht gehören sie aber zu den Guten. Sie nutzen ihr Fachwissen nicht, um Schaden zu verursachen, sondern um ihn zu vermeiden.

Vertrauen entsteht außerdem durch Empfehlungen und Mundpropaganda, sprich: Kundenreferenzen. Outpost24 hat mit seinen PtaaS-Leistungen Unternehmen wie Cezanne HR[6], die Komplett-Gruppe[7] und Lomax[8] überzeugt, ebenso wie EasySignup[9]. Das komplett webbasierte Event-Management-Tool hilft Kunden dabei, Meetings und Konferenzen effizienter zu verwalten und durchzuführen sowie die Daten der Teilnehmer sicher zu verarbeiten. Das Produkt muss jederzeit zur Verfügung stehen, deshalb ist es besonders wichtig, dass potenzielle Sicherheitsprobleme frühzeitig erkannt und behoben werden.

Für das IT-Team des expandierenden Unternehmens EasySignup wurde es zunehmend zu einer Herausforderung, Software-Schwachstellen zu identifizieren, zu schließen und gleichzeitig den täglichen Geschäftsbetrieb aufrechtzuerhalten. Die Firma wandte sich an Outpost24, um eine langfristige und nachhaltige Teststrategie zu entwickeln. Sie sollte sicherstellen, dass alle Schwachstellen identifiziert, protokolliert und untersucht werden. Hinzu kamen Vorgaben der Europäischen Datenschutz-Grundverordnung (DSGVO): EasySignup muss seinen Kunden nachweisen können, dass das Tool persönliche Daten sicher erfasst und verarbeitet. Die Lösung lag in SWAT, einem Angebot für kontinuierliche Tests der Applikation. Damit erkennen EasySignup und Outpost24 Bedrohungen und Risiken frühzeitig rund um die Uhr.

ES LIEGT IN DER NATUR DER SACHE, DASS PENTESTS VERTRAUEN ZUM DIENSTLEISTER VORAUSSETZEN, SCHLIESSLICH WIRD IHM ZUGRIFF AUF SENSIBLE DATEN UND APPLIKATIONEN GEWÄHRT.

[6] **Outpost24:** How Outpost24 helps CezanneHR secure their cloud web application and meet compliance (https://outpost24.com/customers/Cezanne-HR).

[7] **Outpost24:** Redesigning the ecommerce operation for PCI compliance (https://outpost24.com/customers/komplett-group).

[8] **Outpost24:** Ecommerce websites main targets for hackers (https://outpost24.com/customers/lomax).

[9] **Outpost24:** Maintain high availability and avoid business disruption (https://outpost24.com/customers/EasySignUp).

Warum Sie mit PtaaS in die Gegenwart und in die Zukunft investieren

Nahezu alle Prognosen gehen davon aus, dass sich die Bedrohungslage weiter verschärfen wird – für Unternehmen, öffentliche Einrichtungen wie Behörden oder andere Institutionen. Schon heute stehen Menschen alleine dieser Herausforderung hilflos gegenüber. Es braucht Automatisierung und Know-how, um Schwachstellen frühzeitig zu erkennen und zu schließen. PtaaS deckt beides ab, indem es automatische Scans mit manuellen Pentests, also bewährte technische Routinen mit dem Wissen und der Kreativität von Menschen, kombiniert. Dieses Modell überzeugt durch

- seine Flexibilität bei wechselnden Bedarfen,
- konkrete Unterstützung beim Schließen von Schwachstellen,
- bessere Ergebnisse als bei Einzelmaßnahmen,
- das vollständige Aussortieren von Fehlalarmen,
- ein kontinuierliches Monitoring statt einer Stichtagsprüfung,
- große Zeitersparnis, die die Sicherheit drastisch erhöht, weil Lücken viel schneller geschlossen werden als bei klassischen Pentests,
- nutzwertige und verständliche Ergebnisaufbereitung,
- enge Zusammenarbeit der internen Kollegen mit den Sicherheitsexperten von Outpost24 sowie
- Kosteneffizienz und -flexibilität.

Ziel der Cybersecurity ist es, immer schneller zu sein als der Widerpart. Mit PtaaS gelingt Ihnen das wirkungsvoll und kosteneffizient. Es ist der nächste Entwicklungsschritt für jede Organisation, die ihre IT- und Cybersicherheit zeitgemäß, effizient, flexibel und zukunftsfähig aufstellen möchte.

Wer ist Outpost24?

Die Outpost24-Gruppe ist ein führender Anbieter von Cyber-Risk-Management-Lösungen

Die Outpost24-Gruppe ist Vorreiter im Cyber Risk Management mit Angeboten in den Bereichen Vulnerability Management, Application Security Testing, Threat Intelligence und Access Management.

Über 2.500 Kunden in mehr als 65 Ländern vertrauen auf die Lösungen von Outpost24, um Schwachstellen zu identifizieren, externe Bedrohungen zu überwachen und die Angriffsfläche ihrer Organisationen schnell und zuverlässig zu minimieren.

Die Lösungen von Outpost24 werden über unsere Cloud-Plattform bereitgestellt und beinhalten leistungsstarke Automatisierungsfunktionen, deren Ergebnisse von unseren Cybersicherheitsexperten gestützt und bewertet werden. So können sich Organisationen auf die Cyberrisiken konzentrieren, auf die es ankommt.

Ghost Labs

Ghost Labs ist die auf IT-Sicherheit spezialisierte Abteilung von Outpost24, die erweiterte Sicherheitsdienstleistungen wie fortgeschrittene Penetrationstests für Netzwerke, Webanwendungen, Red Teaming und umfassende Exploitation anbietet. Darüber hinaus leistet das Ghost-Labs-Team einen aktiven Beitrag zur Security-Community mit Schwachstellenanalysen und Programmen zur verantwortungsvollen Offenlegung von Schwachstellen.

Ghost Labs führt Hunderte von erfolgreichen Penetrationstests für Kunden, die von globalen Unternehmen bis hin zu KMU reichen, durch. Unser Team besteht aus hoch qualifizierten ethischen Hackern, die ein breites Spektrum an fortschrittlichen Testdienstleistungen abdecken, um Unternehmen dabei zu helfen, mit den sich entwickelnden Bedrohungen und neuen Technologien Schritt zu halten.

Unser Lösungsportfolio

Continuous Cybersecurity Risk Management by Outpost24

- Risk-based Vulnerability Management
- Security-Tests von Webanwendungen und Pentesting as a Service
- Threat Intelligence
- Access Risk und Passwort-Sicherheit
- Managed Security und Professional Services

Kontaktdaten

Patrick Lehnis
Marketingmanager DACH
Mobile: +49 (0) 160 - 348 401 3
E-Mail: Patrick.Lehnis@specopssoft.com
Web: www.specopssoft.com

Specops Software GmbH
Gierkezeile 12 | 10585 Berlin
Tel.: +46-8-465 012 34
Geschäftsführung: Karl Thedéen, Andrea Myrander
Registergericht: Amtsgericht Berlin (Charlottenburg)
Registernummer: HRB 225197 | Ust-ID: DE340100442