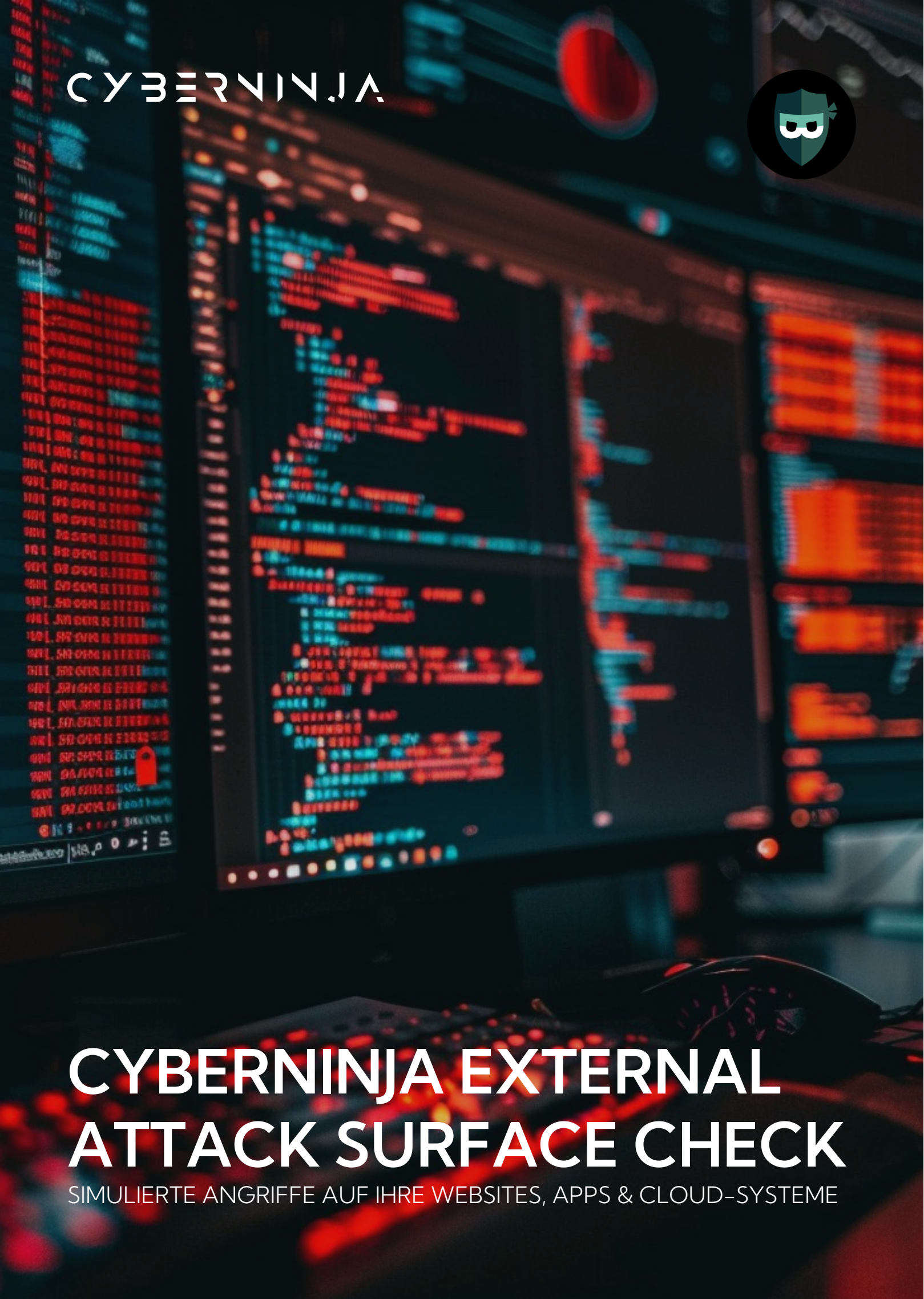

CYBERNINJA EXTERNAL ATTACK SURFACE CHECK

SIMULIERTE ANGRIFFE AUF IHRE WEBSITES, APPS & CLOUD-SYSTEME

RED TEAM SERVICES – WIE SICHER IST IHRE **EXTERNE ANGRIFFSFLÄCHE?**

> Es ist Zeit, nicht mehr auf Annahmen zu vertrauen und zu beweisen, dass Ihre IT-Sicherheit funktioniert.
>
> Unsere internen Hacker greifen Ihre externe Angriffsfläche in Ihrem Auftrag an und zeigen, wie weit ein echter Angreifer kommen könnte.
>
> Roberto Bortoli, CEO

Willkommen beim CyberNinja Red Team

In der heutigen digitalen Welt sind Cyberkriminelle aktiver und raffinierter denn je. Jeden Tag werden Unternehmen weltweit Opfer von Hackerangriffen, Datenlecks und anderen Sicherheitsvorfällen. Die Folgen können verheerend sein: finanzielle Verluste, Reputationsschäden und der Verlust sensibler Daten. Angesichts dieser Bedrohungen ist es entscheidend, dass Ihr Unternehmen proaktiv handelt, um sich zu schützen.

CyberNinja bietet Ihnen umfassende Cyber-Sicherheitsdienstleistungen auf dem neuesten Stand der Technik. Wir kombinieren jahrelange Erfahrung mit modernsten Methoden, um Ihre IT-Infrastruktur zu bewerten und zu schützen. Unsere Experten führen detaillierte Penetrationstests und Vulnerability-Scans durch und simulieren realistische Cyberangriffe durch Red Teaming, um sicherzustellen, dass Ihr Unternehmen bestens auf alle Eventualitäten vorbereitet ist.

Vertrauen Sie auf unsere Expertise. Mit unserem maßgeschneiderten Ansatz helfen wir Ihnen, Ihre Sicherheitslücken zu schließen und Ihre Abwehrkräfte zu stärken. Wir arbeiten eng mit Ihnen zusammen, um sicherzustellen, dass Ihre Systeme nicht nur geschützt, sondern auch resilient gegenüber zukünftigen Bedrohungen sind. Verlassen Sie sich auf unsere Erfahrung und Kompetenz, um Ihr Unternehmen sicher in die Zukunft zu führen.

WAS WIR TUN

1 | ATTACK SURFACE MAPPING (RECONNAISSANCE)

- Wir identifizieren die Angriffsfläche Ihrer Ziele, einschließlich Subdomains, offener Ports und laufender Dienste.
- Wir kartieren Webanwendungstechnologien, machen Screenshots, erkennen WAFs und entdecken versteckte Dateien durch Fuzzing (Google Hacking, verbundene Domains, Subdomains, virtuelle Hosts und mehr).

2 | VULNERABILITY SCANNING

- Wir scannen und erkennen genau häufige Schwachstellen wie XSS, SQLi, OS Command Injections und mehr.
- Wir identifizieren spezifische Sicherheitsprobleme bei API-Schwachstellen und weit verbreiteten CMS wie WordPress, Drupal, Joomla und SharePoint.

3 | EXPLOITATION

- Wir nutzen kritische CVEs aus, verschaffen uns ersten Zugang, extrahieren sensible Dateien und mehr.
- Wir zeigen Ihnen die tatsächlichen Auswirkungen Ihrer Findings, indem wir starke Beweise liefern und Proof-of-Concepts erstellen.
- Wir nutzen auch Web-Schwachstellen wie SQL-Injection, XSS und mehr, um Daten zu extrahieren und reale Sicherheitsrisiken aufzuzeigen.

4 | REPORTING

- Wir erstellen einen benutzerdefinierten, managementfreundlichen Bericht mit allen Details zu den Ergebnissen, einschließlich Beschreibungen, Risiken und Empfehlungen.

OPTIONAL | KONTINUIERLICHE ÜBERWACHUNG

- Wir bieten Ihnen regelmäßige Berichte und auf Abruf eine Management-Präsentation per Videocall. Bei kritischen Sicherheitsvorfällen erhalten Sie sofort eine Benachrichtigung von unserem Security Operation Team.

PREIS UND **UMFANG**

Die Analyse Ihrer externen Angriffsfläche (alles, was direkt über das Internet zugänglich ist) wird von CyberNinja® mithilfe preisgekrönter maschineller Lerntechnologie durchgeführt.

KEY FEATURES

1. **DISCOVERY & MAPPING**
   Wir erstellen eine umfassende Übersicht über all Ihre Anwendungen und APIs, einschließlich solcher, die verloren, nicht dokumentiert oder nicht autorisiert sind. Dank fortschrittlicher Crawling-Techniken und einem kombinierten Scan-Ansatz erkunden wir auch die Ecken Ihrer Webanwendungen und Websites, die andere übersehen könnten.

2. **VULNERABILITY SCANNING**
   Detaillierte Untersuchung aller entdeckten Assets zur Identifizierung potenzieller Schwachstellen, Missbrauchsmöglichkeiten und Sicherheitsrisiken.

3. **EXPLOITATION**
   Ausnutzung kritischer CVEs, Gewinnung des ersten Zugangs, Extraktion sensibler Dateien und mehr, um Ihnen die tatsächlichen Auswirkungen der Ergebnisse zu demonstrieren, durch Bereitstellung von starken Beweisen und Erstellung von Proof-of-Concepts.

4. **REPORT AND RECOMMENDATIONS**
   Erstellung eines detaillierten Berichts mit priorisierten Handlungsempfehlungen.

WAS IST INBEGRIFFEN?

- 1 Website or application of small size and complexity
- Domain- & Subdomain analysis
- Web server security check
- Web software security check (CMS)

WAS WIRD GEPRÜFT?

- Allgemeine Sicherheitsanalyse der Online-Plattform
- Analyse der verwendeten Tools
- Suche nach Schwachstellen im Content-Management-System
- Suche nach ungesicherten Admin-Portalen
- Erkennung von versteckten Klartextinformationen
- Analyse von internen und externen Webanwendungen
- Überprüfung, ob Angreifer sich lateral durch cloud-native Anwendungen bewegen können und auf andere Systeme in Ihrer Cloud zugreifen können
- Umfassende Überprüfung von API-Schnittstellen und Webservices (REST/SOAP)

NACH WELCHEN STANDARDS ARBEITEN WIR?

CyberNinja arbeitet nach globalen Standards:

- OWASP
- NIST SP 800-115
- PCI DSS
- MITRE ATT&CK® Matrix
- ISACA Audit
- CVE / CWE
- CVSS

PREIS

CHF 2’900

Pro OneShot Check einer Domain

OPTIONAL

> Dark Web Exposure Check | EUR 500
> Email Security Check | EUR 1’200
> GDPR & PCI DSS Privacy Check | EUR 900

VORTEILE CYBERNINJA EXTERNER CHECK

TIEFE FALSE POSITIVES RATE

Wir optimieren unseren Ansatz und unsere Tools ständig, um äußerst präzise Ergebnisse zu liefern, sodass Sie keine wertvolle Zeit mit Fehlalarmen verschwenden. Unser Website Vulnerability Scanner validiert automatisch Funde und wendet das Label "Bestätigt" an, wenn das Tool sicher ist, dass die Schwachstelle vorhanden ist.

JAVASCRIPT-SCHWERE WEBSITES

Unser Website Vulnerability Scanner nutzt einen leistungsstarken, browserbasierten Crawler, um Single Page Applications (SPAs) und andere JavaScript-lastige Websites schnell und genau zu scannen. Dieser Ansatz gewährleistet eine umfassende Abdeckung der Angriffsfläche und sorgt für eine hohe Erkennungsrate von Schwachstellen.

AUTHENTICATED SCANNING

Wir bieten auch Scans hinter Login-Seiten an, die Schwachstellen als authentifizierter Benutzer aufdecken. Wir unterstützen mehrere Authentifizierungsmethoden wie Benutzername/Passwort, benutzerdefinierte Header, Cookies und aufgezeichnete Login-Sitzungen.

OUT-OF-BAND DETECTION

Neben klassischen Webanwendungsschwachstellen, die sofort in den HTTP-Antworten sichtbar sind, gibt es auch solche, die nicht auf den Antwortseiten erscheinen. Da sie jedoch Out-of-Band-Anfragen erzeugen, sind wir in der Lage, sie auf diese Weise zu erkennen.

VERTRAUEN AUF **CYBERNINJA** BEDEUTET

REALISTISCHE ANGRIFFSSIMULATION
Unsere Red-Teaming-Dienste simulieren echte Cyberangriffe, um die Reaktionsfähigkeit und Widerstandsfähigkeit Ihres Unternehmens zu testen.

UMFASSENDE SICHERHEITSBEWERTUNG
Wir testen nicht nur die technische IT-Sicherheit, sondern berücksichtigen auch organisatorische und menschliche Faktoren.

ERKENNUNG VON SCHWACHSTELLEN
Wir identifizieren Sicherheitslücken in Ihren Systemen und Prozessen, die durch herkömmliche Methoden möglicherweise übersehen werden.

VERBESSERUNG DER INCIDENT RESPONSE
Wir testen und verbessern die Fähigkeit Ihres Unternehmens, schnell und effektiv auf Sicherheitsvorfälle zu reagieren.

SCHULUNG UND SENSIBILISIERUNG
Wir erhöhen das Sicherheitsbewusstsein Ihrer Mitarbeiter und schulen sie im Umgang mit realistischen Bedrohungsszenarien.

OPTIMIERUNG VON SICHERHEITSMAßNAHMEN
Wir liefern konkrete Empfehlungen zur Verbesserung Ihrer Sicherheitsstrategien und -maßnahmen.

VALIDIERUNG VON SICHERHEITSLÖSUNGEN
CyberNinja® überprüft die Effektivität Ihrer vorhandenen Sicherheitslösungen wie EDR, SIEM und Firewalls.

UNVERZERRTE SICHERHEITSÜBERPRÜFUNG
Wir erstellen ein unverzerrtes Bild Ihrer Sicherheitslage, da Ihr Blue-Team in der Regel nicht über die Simulation informiert ist.

ERFÜLLUNG VON COMPLIANCE-ANFORDERUNGEN
Wir unterstützen Sie bei der Erfüllung gesetzlicher und branchenspezifischer Compliance-Anforderungen durch dokumentierte Sicherheitsüberprüfungen und -verbesserungen.

ÜBER UNS

Als Cyber Security spezialisierter IT-Dienstleister mit Fokus auf das KMU-Kundensegment, kennen wir die Bedürfnisse und Herausforderungen der entsprechenden Unternehmen sehr gut. Durch das gleichzeitige Anbieten von klassischen IT-Services verfügen wir über fundiertes Knowhow, langjährige Erfahrung und Zertifizierungen in den Bereichen Netzwerke, Firewalls, Microsoft 365, Cloudlösungen und Applesysteme. Dadurch sind wir in unserer Hauptdisziplin „CyberSecurity" noch professioneller und effizienter unterwegs. Die heutigen Angriffsvektoren wachsen exponentiell. IT-Sicherheit erfordert immer mehr vernetztes Denken und System-übergreifende Analytik – gerade im KMU-Segment ist es kaum noch möglich, sich auf ein einziges Fachgebiet zu konzentrieren und gleichzeitig umfassende IT-Sicherheit zu garantieren. Wir betreuen Kunden nicht nur im Rahmen von Red-Teaming (Angriffssimulationen), sondern bieten auch entsprechende Schutzsysteme, Incident Response und Forensik (Blue-Teaming). Dank unserem managed Security Operation Center Service stellen wir eine kontinuierliche Überwachung und proaktiven Massnahmen-Umsetzungen IT-Infrastrukturen sicher.

GRÜNDUNG

2014

FOKUS

IT-SECURITY SERVICES

MITARBEITER

8 INTERNE
4 EXTERNE

VISION

Unsere Marke ist Programm: Als CyberNinja's stehen wir Schweizer Unternehmen als Beschützer in der digitalen Welt zur Seite. Unsere Vision ist, IT-Security Services in der Schweiz auch im KMU-Bereich zu etablieren und weiterzuentwickeln. Gerade KMU wissen oft nicht, wie sie im Falle eines Cyberangriffs reagieren sollen bzw. was es braucht, um sich präventiv gegen Cyberangriffe zu wappnen.

SERVICES

CYBERNINJA SHIELD

Umfassende IT- & CyberSecurity Lösung inkl. SOC für KMU

RED TEAM PROFESSIONAL SERVICES

OSINT, CyberSecurity Checks, Penetrationstest, Phishingattacken

BLUE TEAM PROFESSIONAL SERVICES

Managed SIEM / SOC, Cyber Intelligence & Forensic

BEREIT?

KONTAKTIEREN SIE UNS FÜR EIN UNVERBINDLICHES UND KOSTENLOSES GESPRÄCH UNTER **+41 31 529 29 00** ODER AUF **INFO@CYBERNINJA.CH**

Telefon +41 31 529 29 00
Mail info@cyberninja.ch
Web www.cyberninja.ch

Folgen Sie uns #cyberninja

@CYBERNINJA-CH @CYBERNINJA_CH @CYBERNINJA.CH @CYBERNINJA_CH