
CYBERNINJA
SIND SIE BEREIT FÜR
EINEN HACKERANGRIFF?

WIE SICHER IST IHR KMU?

In der Schweiz, wo Innovation und Präzision von zentraler Bedeutung sind, erfordern die Herausforderungen der Cybersicherheit massgeschneiderte und branchenspezifische Lösungen. Schweizer Unternehmen, insbesondere KMUs, sind zunehmend Ziel von Cyberbedrohungen. Die meisten erfolgreichen Angriffe sind auf unbeachtete Sicherheitslücken zurückzuführen.

Finden Sie heraus, ob Ihre Firma gefährdet ist!

Roberto Bortoli, CEO

Willkommen beim CyberNinja Red Team

In der heutigen digitalen Welt sind Cyberkriminelle aktiver und raffinierter als je zuvor. Jeden Tag werden weltweit Unternehmen 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, die auf dem neuesten Stand der Technik basieren. 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. Setzen Sie auf unsere Erfahrung und Kompetenz, um Ihr Unternehmen sicher in die Zukunft zu führen.

> **Wir arbeiten mit Ihrem IT-Partner, nicht gegen ihn.**
>
> Ihr IT-Partner ist ein wichtiger Teil Ihres Unternehmens, das ist uns bewusst. CyberNinja ist nicht hier, um Konkurrenz zu machen, sondern um gemeinsam mit Ihrem IT-Partner das Beste für Ihre Sicherheit herauszuholen. Wir verstehen, dass Vertrauen und Zusammenarbeit der Schlüssel zu einer umfassenden IT-Sicherheit sind, daher unterstützen wir Ihr Team und arbeiten Seite an Seite mit Ihren bestehenden Partnern.

DER **MYTHOS** UND DIE ALARMIERENDE SITUATION FÜR **SCHWEIZER KMU**

" ICH BIN FÜR HACKER UNINTERESSANT!

KÖNNTE DIESE AUSSAGE VON IHNEN STAMMEN?

Tatsache ist, dass Cyberkriminelle in den meisten Fällen die Opfer nicht gezielt aussuchen. Denn sie sind auf Effizienz und hohe Erfolgsquote fokussiert. Genau wie Sie, wollen die Cyberkriminellen mit möglichst wenig Aufwand, möglichst viel verdienen – und möglichst ohne Risiken eingehen zu müssen. Anstatt sich also die Opfer gezielt auszusuchen und damit grössere Risiken einzugehen, verteilen diese Fallen und Köder im Internet, per Emails, SMS oder sie scannen grosse Bereiche des Internets nach einfach zu übernehmenden Systemen.

" FÜR MICH IST DIE INFORMATIK UNKRITISCH

STELLEN SIE SICH FOLGENDE FRAGEN!

Wie sehr wird Ihre Arbeit eingeschränkt, wenn Sie plötzlich keinen Zugriff auf all Ihre Daten haben? Keinen Zugang zu Ihren Aufträgen, zu Ihren Kundenadressen, zu Ihren Mitarbeiterplanungen und Lieferantenbestellsysteme? ?

Wie lang kann Ihr KMU überleben, wenn keines Ihrer Systeme mehr funktioniert? ?

Wie schlimm ist es für Sie, wenn alle Daten, die Sie irgendwo abgespeichert haben, plötzlich publik sind? Was also, wenn all Ihre Kalkulationen von Ihren Mitbewerbern gelesen werden und was wenn Fotos, Passkopien und AHV-Nummern von Ihren Mitarbeitenden im Internet frei heruntergeladen werden können? ?

" MEIN IT-PARTNER HAT ALLES IM GRIFF

VERTRAUEN IST GUT, KONTROLLE IST BESSER!

Natürlich verspricht Ihnen Ihr IT-Partner, das er alles im Griff hat und das Sie keine IT-Sicherheitsüberprüfung notwendig haben. Stimmt das aber auch? Wenn Ihr IT-Partner sich gegen eine Überprüfung sträubt, dann sollten Sie diese erst recht durchführen lassen. Ein vertrauenswürdiger und professioneller IT-Partner empfiehlt Ihnen dies sogar, denn auch er möchte wissen, ob er Lücken übersehen hat. Diese können täglich neu entstehen. Unser Ziel ist es, mit Ihrem IT-Partner zusammen zu arbeiten und ihm zu helfen, Ihre IT sicher zu machen!

DIE DRINGLICHKEIT **VERSTEHEN**

Cyberkriminelle, die meist als grosse Organisationen mit professionellen Strukturen und Prozesse tätig sind, grenzen ihre Zielgruppe ein, um noch erfolgreicher zu sein. Sie fokussieren sich vermehrt auf KMU wie Ihres. Denn diese sind meist nicht so gut geschützt wie Grossunternehmen, haben häufig keine eigene IT-Sicherheitsleute, welche die Systeme kontinuierlich überwachen und haben auch keinen Zugang zu hochprofessionelle und effiziente Abwehrsysteme. Meistens sind nur klassische Antivirenscanner installiert. Datensicherungen werden nach wie vor auf Bänder oder USB-Festplatten gemacht und nie überprüft. Eine kontinuierliche Überwachung und Inventarisierung fehlt gänzlich.

ÜBER 85%
der Systeme und IT-Infrastruktur von KMU werden nicht verwaltet!

ÜBER 90%
der Cyberangriffe beginnen mit einer infizierten E-Mail!

ÜBER 57%
der Angriffe werden von herkömmlichen Virenschutzsysteme nicht erkannt!

ALLE 11 SEK.
wird ein Unternehmen von Ransomware verschlüsselt!

NUR 57%
der Unternehmen gelingt es, Daten mithilfe von Backups wiederherzustellen!

32%
der Ransomware-Opfer bezahlen das Lösegeld, um wieder operativ tätig zu sein!

WIE SIEHTS BEI IHNEN AUS – SIND SIE GEFÄHRDET? WURDEN SIE BEREITS ANGEGRIFFEN UND HABEN ES EINFACH NOCH NICHT BEMERKT?

SIE **BENÖTIGEN** EINE ZUVERLÄSSIGE **SICHERHEITSANALYSE!**

- Die Angriffsfläche in Ihrer IT entwickelt sich ständig weiter
- Jeden Tag werden neue Schwachstellen aufgedeckt
- Kein Unternehmen ist vor Cyberangriffen gefeit
- Sie können nicht hoffen, die Bedrohungen im Griff zu haben, wenn Sie Ihre Schwachstellen nicht kennen

CYBERNINJA **CHECK** BRINGT LICHT INS DUNKLE!

Dank CyberNinja Check kennen Sie einfach, kostengünstig und sicher den aktuellen Zustand Ihrer IT-Sicherheit. Einmalig als Status-Quo Analyse oder als kontinuierliche Statusüberwachung. Dank transparenten und verständlichen PDF-Reports mit entsprechenden Massnahmenempfehlungen, wissen Sie immer, wann, wo und was Sie anpassen müssen, damit Ihr KMU jederzeit auch vor den absolut neusten Gefahren, den sogenannten »ZeroDay» Sicherheitslücken, gut geschützt ist.

CyberNinja kann aber weit mehr als die grundlegende Analyse Ihrer lokalen Informatik. Denn es gilt viel mehr zu schützen, als nur Ihr lokales IT-Netzwerk. Heute werden häufig Cloud-Dienste wie Microsoft 365, Google Workspace und Zoho eingesetzt.

Und nicht selten sind Webseiten nicht nur eine digitale Visitenkarte eines KMU, sondern gehören zu den kritischen und Umsatz bringenden Systemen. Beispielsweise als Onlineshop-Plattform, Terminbuchungssystem, Tisch- oder Zimmerreservationssystem oder als Mitgliederverwaltung.

Häufig werden die digitalen Assets wie Social Media Accounts, Emailadressen und Domainnamen vergessen. In der heute so digitalen Welt, ist es unabdingbar zu wissen, ob Cyberkriminelle Ihre digitale Marke geklont haben, um Ihre potenziellen Kunden auf eine falsche Seite zu locken. Haben Sie das auf dem Radar? Oder wissen Sie, ob vielleicht vertrauliche Daten aus Ihrem Unternehmen im Darkweb gehandelt werden, weil Sie vielleicht bereits kompromittiert wurden und es einfach nicht bemerkt haben?

Und dann war doch da noch was mit dem neuen Datenschutzgesetzt in der Schweiz?

EINFACH, KOSTENGÜNSTIG UND SICHER DEN STATUS QUO IHRER ANGRIFFSFLÄCHE KENNEN

Der CyberNinja Check bietet Ihnen zu allen zentralen Bereichen eine übersichtliche Situationsanalyse.

UMFANG CYBERNINJA CHECK

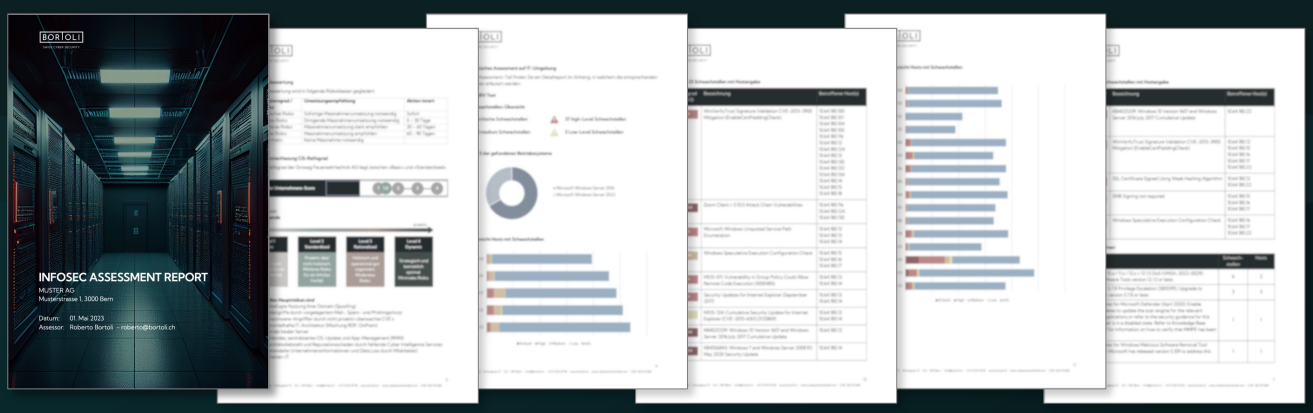
IT SECURITY CHECK

Analyse der Innensicht
Gibt es in Ihrem lokalen Netzwerk Sicherheitslücken und Schwachpunkte?

PROZESSE & RICHTLINIEN

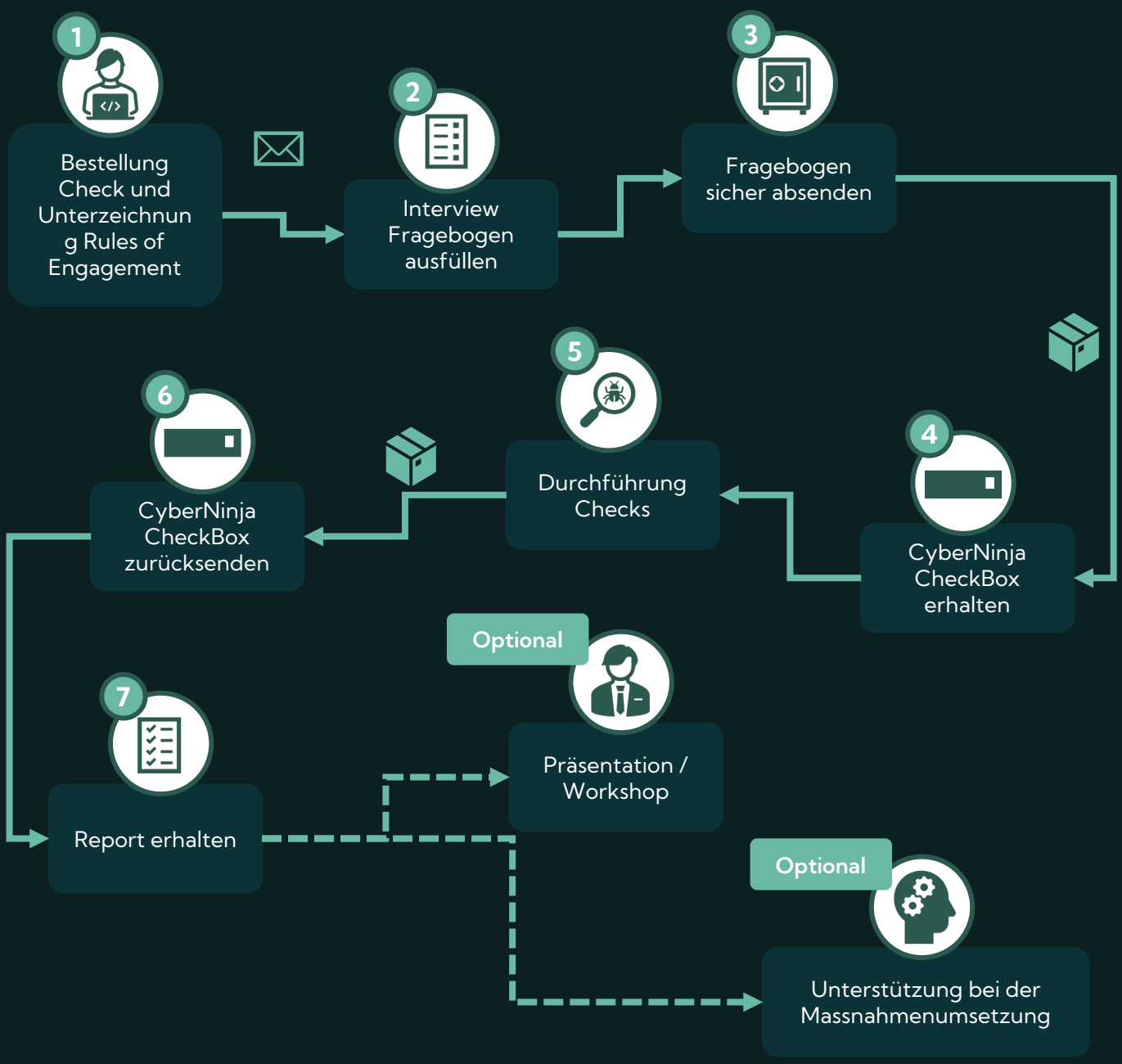
Analyse der Prozesse und Richtlinien
Ist Ihr KMU prozessual richtig aufgestellt? Nach dem CIS-Verfahren prüfen wir Sie mit einem Interview auf Herz und Nieren.

CyberNinja Check erstellt nach jeder Analyse transparente, verständliche und Management taugliche Reports. Diese enthalten das entsprechende Sicherheitsranking, Details zu allen Lücken sowie Massnahmen-Empfehlungen.



WIE LÄUFT EIN CYBERNINJA CHECK AB?

Für die Durchführung eines CyberNinja Checks kommt unsere AttackNode zum Einsatz. Diese muss bei Ihnen ans Netzwerk angeschlossen werden, damit die Analysen durchgeführt werden können. Ganz genau so, wie wenn Sie eine Expertise für eine Bauabnahme machen lassen. Da benötigt der Experte ebenfalls Zutritt zu Ihrem Haus, um den Zustand zu begutachten und eine Expertise erstellen zu können.



WAS UMFASST DER «**IT SECURITY CHECK**» GENAU?

Der IT-Security Check analysiert Ihr lokales Netzwerk und alle am Netzwerk angeschlossenen Geräte wie PC, Notebooks, Drucker, Server, NAS, Telefone, Kameras und IoT-Geräte.

ASSET-DISCOVERY
CyberNinja durchsucht das gesamte Netzwerk und inventarisiert alles. Dabei findet es auch die verstecktesten Systeme wie Web-Kamera, Batch-Systeme und alles andere, was am Netzwerk angeschlossen sein kann.

CYBERSECURITY-ANALYSE
Ein umfassender Scan nach Sicherheitslücken im Netzwerk, deckt offene Türen und Fenster, veraltete Betriebssysteme und versteckten Angriffsflächen auf.

MALWARE-SCAN
Spezifische Suche nach Malware oder Malware-ähnlichen Prozesse sowie und nach Artefakten oder Indizien von möglichen, früheren Angriffen.

ZUGANGSDATEN UND PASSWORT-ANALYSE
Suche nach kompromittierten, unsicheren oder mehrfach genutzte Zugangsdaten, sowie Suche nach, im Klartext abgespeicherten Zugangsdaten auf den Datenablagen.

SICHERHEITSLÜCKEN IN DER EINGESETZTEN SOFTWARE
CyberNinja sucht nach Sicherheitslücken in den Betriebssystemen Ihrer Computer, Server, Drucker und Peripherie-Systeme. Parallel dazu wird nach installierten Applikationen gesucht, die Sicherheitslücken enthalten.

OT SICHERHEITSLÜCKEN
CyberNinja durchsucht auch explizit OT, IOT und ICS-Systeme. Nicht selten sind Geräte wie Überwachungskameras, Telefonieanlagen, Laborgeräte, Röntgensysteme, CNC- und Gerätesteuerungen nicht abgesichert.

Was ist enthalten?
- Bis zu 100 Endpunkte
- Betriebssystem unabhängig
- Check von IoT, OT und SCADA Systeme
- Check von Telefonie und Kameras

WAS UMFASST DER «**PROZESSE UND RICHTLINIEN CHECK**» GENAU?

CyberNinja findet heraus, ob auch prozessuale oder organisatorische Sicherheitslücken und Angriffsmöglichkeiten in Ihrem Betrieb bestehen. Dafür wird die Geschäftsleitung gezielt interviewt und kritische Fragen gestellt. Neben der technischen Gesamtanalyse Ihres KMU, prüfen wir mit dem Security-Interview den Governance-Teil.

Die Interviewfragen ermöglichen uns eine Bewertung im Zusammenhang mit den CIS Controls™ (v8) durchzuführen und einen detaillierteren Einblick in die aktuellen Richtlinien, Verfahren und das Management Ihrer Organisation zu erstellen. Abhängig von Ihrer Strategie, Richtlinien, Risikoappetit und/oder regulatorischen Anforderungen können die Ergebnisse als Orientierungshilfe dienen, welche Themen Ihr Team adressieren sollte, um Ihre Sicherheitsbewertung zu erhöhen.

Was sind die CIS Controls?

Die CIS Controls (früher bekannt unter der Bezeichnung CIS Critical Security Controls) bestehen aus einer Reihe von konkreten Handlungsempfehlungen im Bereich der IT-Sicherheit, um die am weitesten verbreiteten und gefährlichsten Cyberangriffe zu stoppen. Im Mai 2021 wurde die Version 8 der CIS Controls auf der RSA Conference 2021 vorgestellt. Die CIS Controls v8 werden vom Center for Internet Security gepflegt und weiterentwickelt.

Umfang des Interviews

Zu folgenden 18 Punkte (CIS Controls) beantworten Sie in unserem digitalen Fragebogen mittels Multiplechoice-Verfahren Ihren aktuellen Status:

- Inventarisierung der Hardware
- Inventarisierung der Software
- Datensicherheit und Datenschutz
- Sichere Konfiguration
- Benutzerverwaltung
- Rechteverwaltung
- Schwachstellen-Management
- Audit Log Management
- E-Mail- und Webbrowser-Schutz
- Malware-Schutz
- Backups
- Management der Netzwerkinfrastruktur
- Netzwerk-Monitoring
- Security Awareness Training
- Service Provider Management
- Anwendungssoftware-Sicherheit
- Incident Response Management
- Penetration Testing

VORTEILE DES CYBERNINJA CHECKS

- Einzigartige, volldigitalisierte und automatisierte Checks
- Umfassende Checks, die nicht nur die IT-Umgebung, sondern auch Ihre Prozesse und Ihr Umgang mit der Informatik umfassen
- Keine komplexe Installation notwendig. Geführter Check dank benutzerfreundlicher CyberNinja Check Box
- Keine fremden Personen in Ihrem Betrieb
- Sie entscheiden, wann, wieviel und was getestet werden soll
- Als Einmalcheck oder als kontinuierlicher Check erhältlich
- Zugang zu transparente, für Jeden verständliche Dokumentationen nach jedem Check über das OnlinePortal, inklusive Massnahmenempfehlungen und Umsetzungstipps
- Bei Bedarf Remoteunterstützung für die Massnahmenumsetzung sowie online Workshops für das Kader und Mitarbeiter

FÜR WEN SIND DIE CYBERNINJA CHECKS INTERESSANT?

- **KMU INHABER UND GL**
  Effizientes Risikomanagement dank Kennen und Verstehen der eigenen Schwachstellen. Dadurch auch Kontrolle des eigenen IT-Partner möglich.
- **VERSICHERUNGEN**
  Dank transparenter Informationen über den Zustand der kundenseitigen Informatik, können die Risiken besser abgeschätzt und Policen gewinnbringender ausgestellt werden.
- **IT-SERVICE ANBIETER**
  Neue Aufträge, bessere Beratungen und gewinnbringendere SLA's dank fundierten Wissens über den Status Quo der installierten Informatikumgebung.

WAS KOSTET DER «**CYBERNINJA CHECK**»?

CyberNinja hat eine transparente und überschaubare Preisstruktur. Keine komplexen Berechnungen, keine versteckten Kosten und keine schlechten Überraschungen. Wählen Sie zwischen einer einmaligen Analyse zur Standortbestimmung oder einer wiederkehrenden Analyse zur langfristigen Überwachung Ihrer IT-Sicherheit.

EINMALIGER CHECK

CHF **3'990.–**

- ✓ inkl. IT-Security Check (bis zu max. 100 Endpunkte)
- ✓ inkl. Prozesse und Richtlinien Check
- ✓ inkl. einfacher Darkweb Kurzcheck
- ✓ 7 Tage Analysezeit
- ✓ CyberNinja CheckBox
- ✓ Versicherungstauglicher Report
- ✓ Durchgeführt durch CyberNinja, ein regionales Schweizer Unternehmen. Datenschutzkonform und mit höchsten Qualitätsstandards.

Optional: Management Beratung

CHF **450**

Persönliche Besprechung der Analyse und Präsentation.
1 Stunde - Online.

Alle Preise in CHF und exkl. Mehrwertsteuer. Unterstützung bei der Umsetzung der Massnahmenempfehlungen ist nicht inkludiert und wir wird bei Bedarf separat offeriert.

VORAUSSETZUNGEN FÜR DEN CYBERNINJA CHECK

VORBEREITUNG DER INFORMATIK

Damit der Check effizient, sicher und ohne Unterbruch Ihres Tagesgeschäftes durchgeführt werden kann, ist eine ordentliche Vorbereitung unabdingbar. Das wichtigste dabei ist, dass sichergestellt wird, dass alle relevanten Endpunkte eingeschaltet und am Netzwerk angeschlossen sind. Wir können nur prüfen, was in Betrieb ist.

ADMINISTRATOR-ZUGANG

Je nachdem, ob optional auch Cloud-Umgebungen getestet werden sollen, benötigen wir Administratorenrechte zu Ihren Cloud-Diensten (Azure, M365, Google). Sie können uns hierfür einen neuen, temporären Admin-User eröffnen, oder die Zugangsdaten zum bestehenden geben.

INFORMATION AN IHREN IT-PARTNER

Es ist wichtig, dass Ihre IT-Partner informiert werden. Es kann sein, dass die CyberNinja Checks bei eingerichteten Überwachungsmechanismen Alarm auslösen. Wenn dies geschieht, dann ist das schon ein gutes Zeichen. Damit dieser aber nicht überrascht wird, ist es empfehlenswert, ihn zu informieren.

INTERNETZUGANG OHNE PROXY-SERVER

Damit wir Cloud-Dienste prüfen können, benötigen wir einen direkten Zugang ohne Proxy-Server.

IHRE ANWESENHEIT IST NICHT NOTWENDIG

Sie müssen während der Checks nicht anwesend sein und sich voll und ganz Ihrem Tagesgeschäft widmen. Die CyberNinja AttackNode läuft völlig autonom, wird aber durch unsere Spezialisten während der Checks überwacht. So wird sichergestellt, dass alles rund läuft und Sie und Ihre IT nicht gestört werden.

HÄUFIG GESTELLTE FRAGEN – **FAQ**

? BASIERT DAS BASIS ASSESSMENT VON CYBERNINJA AUF EINER CLOUD-ANWENDUNG?

Nein, es wird eine «AttackNode» im IT-Netzwerk des Kunden installiert. Alle gesammelten Daten bleiben innerhalb des Kundennetzwerks.

? WER HAT ZUGANG ZU DEN DATEN, DIE GESAMMELT WERDEN?

Nur der Kunde selbst und unsere Infosec-Engineers, die den IT Security Check durchführen, haben Zugriff auf die gesammelten Daten. Die CyberNinja AttackNode wird bei Ihnen vor Ort eingesteckt, es werden keine Daten an Dritte oder in einen Cloud-Speicherort transferiert. Die CheckBox wird nach der Auswertung aller Daten und der Abgabe des Berichtes komplett gelöscht.

? VERWENDET CYBERNINJA MEINE UNTERNEHMENSDATEN FÜR ANDERE ZWECKE ALS EINE CYBERSICHERHEITSBEWERTUNG?

Nein, die CyberNinja AG verwendet die in den Security Checks gewonnenen Daten nur für die Erstellung und Auswertung der Sicherheitsanalyse. Die Daten werden bei uns auch nicht gespeichert. Im Falle eines Verlustes, muss ein Check erneut durchgeführt werden. Die IT-Security Reports werden in unserem Kundensystem als PDF-Datei verschlüsselt abgelegt.

? INSTALLIERT CYBERNINJA ETWAS AUF DEN ENDPUNKTEN?

CyberNinja installiert keinen permanenten Agenten auf Endpunkte wie PC oder Server. Unsere CyberNinja AttackNode führt alle Analysen direkt aus.

? WAS IST MIT DEM NETZWERKVERKEHR? VERURSACHT CYBERNINJA BEIM CHECK LEISTUNGSPROBLEME IM NETZ?

Nein, die Tests werden in einer Stufe durchgeführt, die den normalen Datenverkehr nicht stört. In seltenen Fällen kann es vorkommen, dass ein Drucker Hieroglyphen ausdruckt, während er analysiert wird. Gerade bei älteren Modellen ist das schon vorgekommen. Unsere IT Security Spezialisten überwachen die Arbeit der AttackNode während der Analysen. Sollte festgestellt werden, dass unerwartet und aufgrund eines Checks ein erhöhtes Datenvolumen generiert wird, wird der Test abgebrochen.

? WIRD EIN ÜBERWACHUNGSTOOL EINGESETZT?

Nein, CyberNinja erstellt nur eine Momentaufnahme des aktuellen Zustandes Ihrer Cybersicherheit. CyberNinja sammelt relevante Informationen, indem es Daten von Endpunkten (Windows-Laptops/Desktops und Windows-Servern), Office 365-Diensten, Azure AD und lokalem Active Directory extrahiert. Darüber hinaus verwenden wir einen Fragebogen, um Einblicke in die Unternehmensrichtlinien und -verfahren im Bereich Cybersicherheit zu erhalten.

HÄUFIG GESTELLTE FRAGEN – **FAQ**

? WIE ERHALTE ICH DIE CYBERNINJA CHECKBOX

Die Box wird Ihnen per Post zugesendet, nachdem Sie die Bestellung ausgeführt und den Interviewfragebogen ausgefüllt haben. Ab Versand haben Sie 7 Tage Zeit, die Checks durchführen zu lassen. Danach müssen Sie die CheckBox mit der vorfrankierten Box wieder zurücksenden. Eine Nachverrechnung bei verspätetem Rückversand behalten wir uns vor.

? GIBT ES VERSTECKTE KOSTEN ODER VERTRAGSLAUFZEITEN?

Nein. CyberNinja bietet transparente und einfache Kostenstrukturen. Keine Überraschungen, Sie bezahlen nur für das, was Sie gebucht haben.

? BIETET CYBERNINJA EINE BERATUNG NACH DEM CHECK?

Ja. Sie haben die Möglichkeit zu jedem Check eine optionale, einstündige Beratung zu buchen. In dieser erklären wir Ihnen die Resultate und können auf Wunsch, auch eine Managementpräsentation für Ihre Geschäftsleitung oder den Verwaltungsrat durchführen.

? WIESO MUSS ICH MEINE KENNWORT ABGEBEN. EIN HACKER HAT DIESE JA AUCH NICHT.

Mit dem CyberNinja Check führen wir keinen Penetrationstest durch und versuche somit nicht, in Ihr System einzudringen. CyberNinja Check erstellt eine Expertise Ihrer IT-Anlage mit Fokus auf die IT-Sicherheit. Ganz genau so, wie wenn Sie eine Expertise für eine Bauabnahme machen lassen. Da benötigt der Experte ebenfalls Zutritt zu Ihrem Haus, um die Analysen durchführen und eine Expertise erstellen zu können.

? MEIN AKTUELLER IT-BETREUER RATET MIR VON DIESEM TEST AB.

Ob Sie einen IT-Sicherheitstest in Ihrem Unternehmen machen lassen wollen, oder nicht, sollte nicht Ihr aktueller IT-Partner entscheiden. Wenn dieser vor einer Expertise abrät, dann sollte man sich überlegen, wieso er sich davor fürchtet. Mit den CyberNinja Checks werden Fehlkonfigurationen, Sicherheitslücken und vergessene Einstellungen aufgedeckt. Das hilft Ihnen, Ihr System sicher zu halten und Ihr IT-Partner erhält die Möglichkeit, das System weiter zu optimieren.

Ausserdem ist ein CyberSecurity Check heute häufig auch notwendig, um eine CyberPolice bei einer Versicherung zu erhalten. Ohne eine fundierte Analyse der IT-Anlage wird das Risiko der Police hoch eingestuft und die Police wird entweder teuer oder gar nicht abschliessbar.

OPTIONALE AUDITS ZUR ERWEITERTEN SICHT AUF IHRE INFORMATIK-SICHERHEIT

Mit einem CyberNinja CHECK kennen Sie die Ist-Situation Ihrer Informatiksicherheit. Dank unserer zusätzlichen, erweiterten Audits prüfen Sie nicht nur Ihre Informatikinfrastruktur, sondern auch Ihre Mitarbeiter, Ihre Datenschutzsituation und finden heraus, ob allenfalls bereits kritische Daten von Ihnen im Umlauf sind oder gar gehandelt werden.

PHISHING SIMULATIONEN

Mit E-Mails, die sich nicht von den Phishing E-Mails der Cyberkriminellen unterscheiden, trainieren wir Ihre Belegschaft. Damit Ihre Mitarbeitenden zu den stärksten Verteidigern gegen die unsichtbare Gefahr von Hackern werden.

DATENSCHUTZ CHECK

Sind Sie und Ihre Webseite bezüglich des Schweizer Datenschutzgesetzes vom 1. September 2023 gerüstet? In Zusammenarbeit mit der Onlaw GmbH wird Ihr Unternehmen auf Datenschutzthemen überprüft.

CYBER INTELLIGENCE

Ist Ihre Marke, Ihre Social Media Accounts oder Ihre Domain sicher? Oder sind diese geklont worden und werden gerade missbraucht? Sind Ihre Daten bereits im Umlauf? Wir finden es für Sie heraus.

PENETRATIONS TESTS

Mit Penetrationstests greifen wir Ihre Infrastruktur und Applikationen gezielt an. Im Gegensatz zu den CyberNinja Checks zeigen wir die Sicherheitslücken nicht nur auf, sondern nutzen diese aus und prüfen, wie weit wir kommen. Bringen wir Ihre gesamte Informatiksysteme in unsere Gewalt? Dann sind dringende Massnahmenumsetzungen notwendig!

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