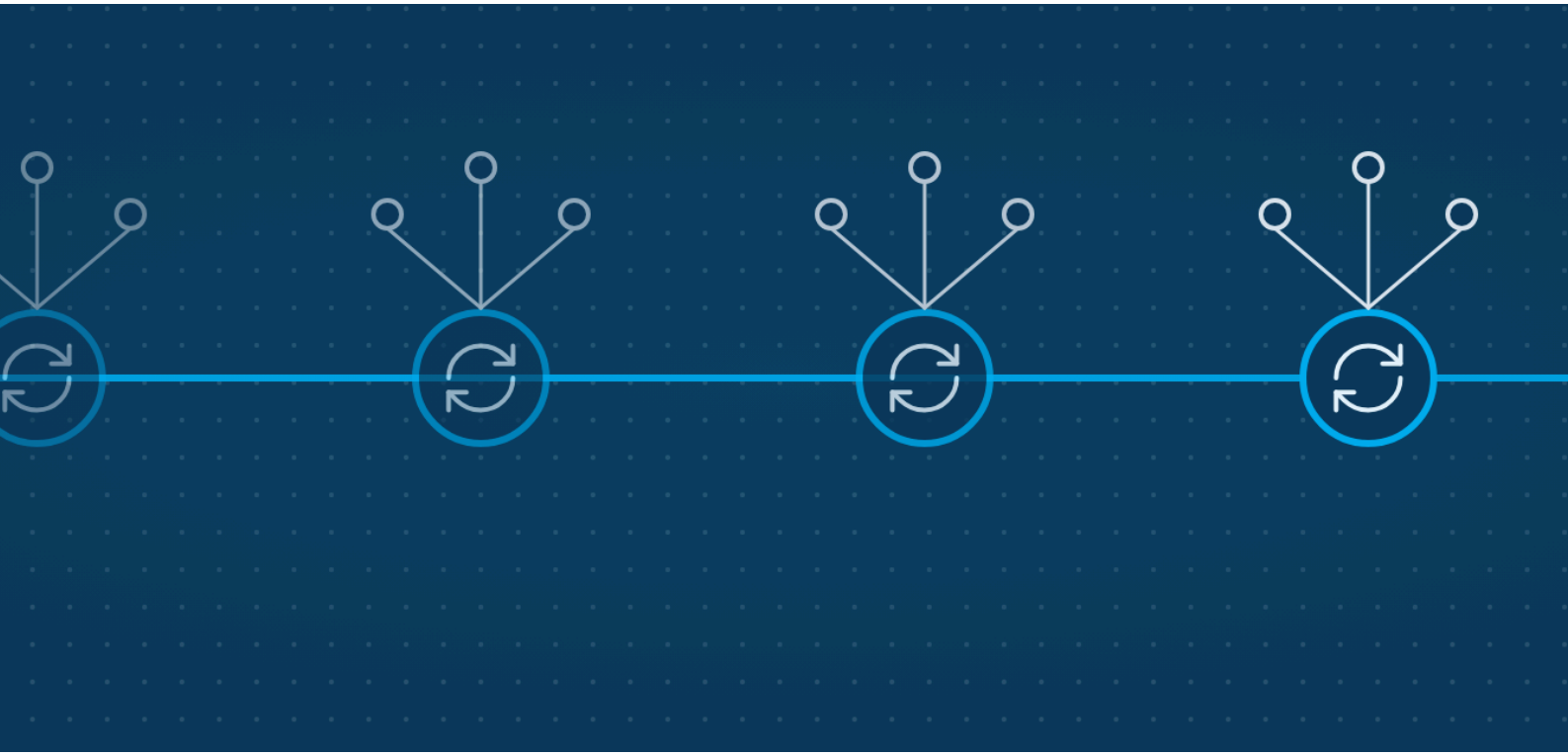
n-komm.
Unser IT Partner

Whitepaper

Pentest manuell und automatisiert: Tiefe und Wiederholung verbinden

Was manuelle Penetrationstests und automatisiertes Pentesting mit Pentera leisten und wie Sie beides kombinieren.



n-komm GmbH · Karlsruhe · Stand November 2026

Auf einen Blick

Was manuelle Penetrationstests und automatisiertes Pentesting mit Pentera leisten und wie Sie beides kombinieren.

- Ein Penetrationstest ist ein kontrollierter Angriff mit Ihrer Erlaubnis. Er zeigt nicht nur, wo Lücken sind, sondern welche sich ausnutzen lassen und zu welchen Angriffswegen sie sich verbinden.
- Der manuelle Pentest ist stark in Tiefe und Kreativität, etwa bei Webanwendungen, besonderen Systemen und komplexen Szenarien. Er ist aber eine Momentaufnahme.
- Automatisiertes Pentesting prüft wiederholt und nach jeder größeren Änderung. Es zeigt die ausnutzbaren Angriffswege priorisiert und macht den Verlauf Ihrer Sicherheitslage sichtbar.
- Beides ersetzt sich nicht, sondern ergänzt sich: der manuelle Test für die Tiefe, das automatisierte Pentesting für die Wiederholung dazwischen.
- Ob Sie eine Plattform selbst betreiben oder als Managed Service nutzen, hängt vor allem davon ab, wer bei Ihnen die Ergebnisse abarbeitet. Ein späterer Wechsel ist möglich.

Inhalt

1. Warum Sicherheitsmaßnahmen geprüft werden müssen
2. Der manuelle Penetrationstest: Tiefe durch Erfahrung
3. Automatisiertes Pentesting: Wiederholung als Prinzip
4. Wie sich beide Ansätze ergänzen
5. Selbst betreiben oder testen lassen?
6. Wie die n-komm unterstützt
7. Checkliste: Pentest-Strategie festlegen

01

Warum Sicherheitsmaßnahmen geprüft werden müssen

Firewall da, Virenschutz da, Passwortregeln da. Ob das alles einem echten Angriff standhält, weiß in vielen Unternehmen und Verwaltungen niemand genau. Oft genügt Angreifern eine falsch gesetzte Firewall-Regel, ein Testserver, an den keiner mehr denkt, oder ein Benutzerrecht, das zu weit gefasst ist.

Die eigene IT-Abteilung sieht solche Stellen im Alltag selten. Sie kennt ihre Systeme sehr gut und schaut als Verteidiger darauf. Ein Angreifer sucht dagegen genau die Stellen, an die niemand gedacht hat, und verbindet kleine Schwächen zu einem großen Angriffsweg. Ein Angriffsweg ist die Kette von Schritten, über die ein Angreifer von einem ersten Zugang bis zu seinem Ziel kommt, etwa zu Administratorrechten oder sensiblen Daten.

Dazu kommt die Pflicht zum Nachweis. NIS2 verlangt von betroffenen Organisationen, und ISO 27001 von zertifizierten, dass sie die Wirksamkeit ihrer Sicherheitsmaßnahmen bewerten. Auch Versicherungen und große Kunden fragen nach. Ein Prüfbericht aus einem Penetrationstest liefert dafür einen belastbaren Beleg.

Und schließlich verändert sich jede IT laufend. Ein neuer Server geht in Betrieb, ein Dienstleister bekommt einen Zugang, für ein Projekt wird eine Firewall-Regel geöffnet und danach vergessen. Jede dieser Änderungen kann einen neuen Angriffsweg schaffen. Eine Prüfung, die einmal stattgefunden hat, sagt deshalb wenig darüber, wie sicher Ihre IT heute ist.

Für IT-Leitung und Geschäftsführung ergeben sich daraus zwei Fragen. Erstens: Wie gut hält unsere IT einem gezielten Angriff stand, und welche Lücken sind wirklich gefährlich? Zweitens: Wie behalten wir diesen Stand im Blick, wenn sich die IT weiter verändert? Der manuelle Penetrationstest beantwortet vor allem die erste Frage, das automatisierte Pentesting vor allem die zweite. Die folgenden Kapitel zeigen, was beide Ansätze leisten und wie sie zusammenpassen.

Kurz erklärt: drei Arten der Prüfung

Ein Schwachstellenscan findet bekannte Lücken automatisch, oft Hunderte, ohne zu prüfen, ob sie sich ausnutzen lassen. Ein Penetrationstest (Pentest) prüft von Hand, ob sich Lücken tatsächlich ausnutzen lassen und wie weit ein Angreifer damit kommt. Automatisiertes Pentesting überträgt diesen Ansatz auf eine spezialisierte Plattform, die Angriffe wiederholbar nachstellt.

02

Der manuelle Penetrationstest: Tiefe durch Erfahrung

Bei einem Penetrationstest versuchen Sicherheitsexperten gezielt, Schwachstellen in Ihrer IT auszunutzen. Sie gehen vor wie echte Angreifer, allerdings mit Ihrer schriftlichen Erlaubnis und in einem vorher festgelegten Rahmen. Systeme, Testart, Ziele und Testzeiten werden vorab vereinbart, ebenso Ansprechpartner und Notfallregeln.

Wie viel ein Test bringt, entscheidet sich schon vor dem Start. Formulieren Sie klare Ziele: Kommt ein Angreifer aus dem Internet in Ihr Netz? Wie weit kommt er von einem infizierten Notebook aus? Lassen sich Daten aus einer Webanwendung abgreifen? Binden Sie Geschäftsleitung, IT und die Verantwortlichen der betroffenen Systeme früh ein, bei ausgelagerten Systemen auch den Dienstleister. Ein klar abgegrenzter Umfang setzt das Budget dort ein, wo das Risiko am größten ist.

Der Unterschied zum Schwachstellenscan liegt in der Handarbeit. Die Tester prüfen, ob sich gefundene Lücken wirklich ausnutzen lassen, und verbinden einzelne Schwächen zu realistischen Angriffswegen. Dabei folgen sie auch ungewöhnlichen Ideen, die keine Software vorhersieht. So erfahren Sie nicht nur, dass es ein Problem gibt, sondern auch, wie gefährlich es ist.

Welche Testart sinnvoll ist, hängt davon ab, was Sie schützen wollen. Ein externer Test greift die Systeme an, die aus dem Internet erreichbar sind, etwa Firewall, Homeoffice-Zugänge und Mailserver. Ein interner Test geht davon aus, dass ein Angreifer bereits im Netz ist, zum Beispiel über ein infiziertes Notebook, und prüft auch das Active Directory, also den zentralen Verzeichnisdienst für Benutzer und Rechte. Weitere Prüfungen richten sich auf Webanwendungen und Schnittstellen, Microsoft 365 und Cloud-Umgebungen, WLAN oder gezielte Täuschungsversuche gegenüber Beschäftigten (Social Engineering).

Wie viel die Tester vorab wissen, wird ebenfalls festgelegt. Fachleute unterscheiden drei Ansätze, die sich in Aufwand und Erkenntnisgewinn voneinander abheben.

Das Ergebnis ist ein Bericht mit zwei Teilen: einer Zusammenfassung für die Geschäftsleitung und einem technischen Teil für die IT. Jede Schwachstelle ist nach ihrem Risiko bewertet und mit einer konkreten Empfehlung versehen. Kritische Funde sollten ohne Verzug gemeldet werden, nicht erst im Abschlussbericht. Ein Nachtest zeigt anschließend, ob die Maßnahmen wirken.

Die Grenze des manuellen Tests ist die Zeit. Er zeigt Ihre IT an einem bestimmten Stichtag. Ihn sehr viel häufiger zu wiederholen, ist aufwendig. Sinnvoll ist ein erneuter Test nach Ihrem Risiko und nach wesentlichen Änderungen an Anwendungen, Netzen oder Systemen.

- Black-Box-Test: Die Tester erhalten keine Informationen über Ihre Systeme und greifen an wie Außenstehende.
- Grey-Box-Test: Die Tester kennen einige Details, zum Beispiel ein normales Benutzerkonto. So zeigt sich, was ein Angreifer mit gestohlenen Zugangsdaten erreicht.
- White-Box-Test: Die Tester erhalten umfassende Informationen, etwa Netzpläne oder Quellcode, und finden so in kurzer Zeit auch versteckte Schwachstellen.

03

Automatisiertes Pentesting: Wiederholung als Prinzip

Beim automatisierten Pentesting prüft eine spezialisierte Plattform Ihre IT-Umgebung auf mögliche Angriffswege. Sie geht vor wie ein Angreifer: Sie sucht Schwachstellen, versucht sie auszunutzen und prüft dann, wie weit ein Angreifer von dort aus käme. Sie stellt zum Beispiel fest, ob sich Passwörter abgreifen lassen und ob sich ein Angreifer im Netz von System zu System bewegen kann. Fachleute nennen diese Bewegung laterale Bewegung.

Damit unterscheidet sich automatisiertes Pentesting deutlich vom Schwachstellenscan. Ein Scanner meldet alle Lücken, die er findet. Die Plattform zeigt dagegen, welche Lücken sich tatsächlich ausnutzen lassen und welche Angriffswege daraus entstehen. Sie ordnet die Funde selbst danach, wie weit ein Angreifer über sie kommt. Ihre IT sieht so auf einen Blick, wo sie anfangen sollte.

Der eigentliche Vorteil liegt in der Wiederholung. Weil die Tests automatisiert laufen, lassen sie sich so oft wiederholen, wie es Ihr Risiko verlangt, etwa nach dem Patchday, nach einer neuen Firewall-Regel oder nach dem Anschluss eines Standorts. Wer eine Lücke geschlossen hat, kann erneut testen und sieht, ob die Maßnahme greift.

Gerade für Organisationen ohne eigenes Sicherheitsteam ist diese Priorisierung wertvoll. Statt einer langen Liste von Funden aus dem Scanner erhalten sie eine überschaubare Reihenfolge: Welche Lücke öffnet den Weg zu Administratorrechten, welche führt zu sensiblen Daten, welche ist zwar vorhanden, aber für einen Angreifer kaum nutzbar? So fließt die knappe Zeit der IT zuerst in die Maßnahmen mit der größten Wirkung.

Im Vergleich der Berichte wird außerdem der Verlauf sichtbar. Sie erkennen, wie sich Ihre Sicherheitslage über die Zeit entwickelt, und können diese Entwicklung gegenüber Geschäftsleitung, Prüfern oder Versicherung belegen. Das unterstützt die Bewertung der Wirksamkeit, die NIS2 und ISO 27001 verlangen.

Für den Einstieg empfiehlt sich eine erste Prüfung als Bestandsaufnahme. Sie zeigt den aktuellen Stand und die Angriffswege, die heute bestehen. Aus den Ergebnissen entsteht eine Liste priorisierter Maßnahmen. Jede weitere Prüfung zeigt dann, ob die Maßnahmen wirken und ob neue Lücken hinzugekommen sind.

Auch automatisierte Tests greifen in die laufende IT ein. Deshalb gehören Umfang, Freigaben und Testfenster vorab festgelegt, und besonders kritische Systeme lassen sich ausnehmen. Ein Restrisiko für den Betrieb sollte im Vorgespräch offen angesprochen werden.

Die Grenze liegt in der Kreativität. Eine Plattform prüft vor allem Netzwerk, Infrastruktur und Cloud und folgt bekannten Angriffstechniken. Individuelle Webanwendungen, besondere Systeme und ungewöhnliche Angriffsideen bleiben die Domäne erfahrener Tester.

Kurz erklärt: Momentaufnahme oder Verlauf

Ein manueller Pentest ist wie ein Foto: Er zeigt Ihre IT sehr genau an einem Tag. Automatisiertes Pentesting ist eher eine Bildserie: Jeder Test zeigt den aktuellen Stand, und im Vergleich sehen Sie, ob neue Angriffswege entstanden sind und ob Ihre Maßnahmen wirken.

04

Wie sich beide Ansätze ergänzen

Automatisiertes Pentesting ersetzt den manuellen Penetrationstest nicht, und umgekehrt reicht ein einzelner manueller Test nicht, um eine sich ständig ändernde IT im Blick zu behalten. Beide Ansätze beantworten unterschiedliche Fragen. Der manuelle Test fragt, wie weit ein erfahrener Angreifer mit eigenen Ideen kommt. Das automatisierte Pentesting fragt, ob seit dem letzten Test neue Angriffswege entstanden sind.

In der Praxis bewährt sich deshalb die Kombination: ein manueller Pentest für die Tiefe, etwa für Webanwendungen, besondere Systeme und komplexe Szenarien, und automatisiertes Pentesting für die Wiederholung dazwischen. Ein vorhandener Schwachstellenscanner bleibt dabei nützlich, weil er die Breite abdeckt.

Eine sinnvolle Reihenfolge beginnt oft mit einer ersten Prüfung, aus der eine Liste priorisierter Maßnahmen entsteht. Danach geht es um das Schließen der Lücken und um die Frage, ob die Maßnahmen wirken. Genau hier spielt die Wiederholung ihre Stärke aus.

Wie oft getestet wird, richtet sich nach Ihrem Risiko, einen allgemein richtigen Zyklus gibt es nicht. Maßgeblich sind die Bedeutung der Systeme, die Häufigkeit von Änderungen und die Anforderungen von Aufsicht, Prüfern oder Kunden. Wichtiger als ein fester Termin ist die Regel, nach wesentlichen Änderungen erneut zu prüfen: nach dem Anschluss eines Standorts, der Einführung einer neuen Anwendung oder dem Umbau des Netzes.

Auch für Nachweise ergänzen sich beide Ansätze. Der Bericht eines manuellen Tests dokumentiert eine gründliche Prüfung zu einem Zeitpunkt. Die wiederkehrenden Berichte aus dem automatisierten Pentesting belegen, dass Sie Ihre Maßnahmen laufend kontrollieren und Lücken nachweisbar schließen.

Für Verwaltungen und Unternehmen mit knappen Ressourcen hat die Kombination noch einen Vorteil. Der aufwendigere manuelle Test wird gezielt dort eingesetzt, wo Kreativität gefragt ist. Die regelmäßige Kontrolle der Infrastruktur übernimmt die Plattform. So entsteht ein Prüfprogramm, das die Tiefe nicht vernachlässigt und trotzdem zeitnah zeigt, ob neue Angriffswege entstanden sind.

- Manueller Pentest als Startpunkt oder bei neuen Anwendungen und wesentlichen Umbauten.
- Lücken nach Risiko schließen, die kritischen zuerst.
- Automatisiert nachprüfen, ob die Maßnahmen wirken.
- Im festgelegten Rhythmus und nach größeren Änderungen wiederholen.
- Berichte vergleichen und als Nachweis nutzen.

	Manueller Penetrationstest	Automatisiertes Pentesting
Wer prüft	Experten, von Hand	spezialisierte Plattform
Stärke	Tiefe, Kreativität, individuelle Angriffsideen	Wiederholbarkeit, schnelle Ergebnisse
Geeignet für	Webanwendungen, besondere Systeme, komplexe Szenarien	Netzwerk, Infrastruktur, Cloud, Wirksamkeitskontrolle
Einsatz	gezielt, nach Risiko und bei wesentlichen Änderungen	wiederholt, im Rhythmus nach Risiko und nach Änderungen
Ergebnis	ausführlicher Bericht zu einem Zeitpunkt	priorisierte Angriffswege und Verlauf über die Zeit

05

Selbst betreiben oder testen lassen?

Wer sich für automatisiertes Pentesting entscheidet, steht vor einer zweiten Frage: Wer fährt die Tests? Mit einer eigenen Lizenz läuft die Plattform im eigenen Rechenzentrum, und das eigene Team startet die Tests. Im Managed Service übernehmen die Experten eines Dienstleisters Planung, Durchführung und Auswertung. Die Technik ist in beiden Fällen dieselbe, der Unterschied liegt in der Arbeit, die bei Ihnen bleibt.

Eine eigene Lizenz bietet die größte Freiheit. Ihr Team testet, wann es will, und sieht neue Angriffswege zeitnah statt erst beim nächsten Termin. Das Wissen über Angriffe wächst im eigenen Haus. Die Kehrseite: Wer ständig testen kann, muss auch ständig reagieren. Jeder Test liefert Funde, die jemand einordnen und abarbeiten muss. Fehlt die Zeit dafür, bleiben Lücken offen, obwohl sie bekannt sind.

Der Managed Service setzt kein eigenes Sicherheitsteam voraus. Sie erhalten nach jedem Test einen Bericht und eine Besprechung mit klaren Prioritäten, verständlich auch für die Geschäftsleitung. Dafür wird nicht laufend geprüft, sondern im vereinbarten Rhythmus. Lücken, die zwischen zwei Terminen entstehen, zeigt erst der nächste Test, und ein zusätzlicher Test nach einer größeren Änderung muss abgestimmt werden.

Unabhängig vom Modell gilt: Das Schließen der Lücken ist eine eigene Aufgabe. Klären Sie früh, wer sie übernimmt, Ihr Team oder ein Dienstleister, und wie Sie die Wirkung prüfen.

Prüfen Sie ehrlich, wer bei Ihnen welche Aufgabe übernimmt. Mit eigener Lizenz plant Ihr Team die Tests, legt Umfang und Ausnahmen für kritische Systeme fest, ordnet die Ergebnisse ein und betreibt die Plattform. Im Managed Service bereitet der Dienstleister vor, Sie geben frei, und die Prioritäten werden gemeinsam in der Ergebnisbesprechung festgelegt. Die Entscheidung über Maßnahmen und Budget bleibt in beiden Fällen bei IT-Leitung und Geschäftsführung.

Die Wahl muss nicht endgültig sein. Ein möglicher Weg: mit dem Managed Service starten, Ergebnisse und Abläufe kennenlernen und später auf eine eigene Lizenz wechseln, wenn das eigene Team so weit ist. Achten Sie bei der Auswahl darauf, dass ein solcher Wechsel vertraglich möglich ist.

	Eigene Lizenz	Managed Service
Wie oft getestet wird	jederzeit, auch nach jeder Änderung	im vereinbarten Rhythmus
Wer testet	Ihr Team	Experten des Dienstleisters
Wer einordnet und berichtet	Ihr Team, auf Basis der priorisierten Funde der Plattform	der Dienstleister, mit Bericht und Besprechung
Wo die Plattform läuft	im eigenen Rechenzentrum	Betrieb liegt nicht bei Ihnen
Was Sie intern brauchen	Personal mit Sicherheitswissen und feste Zeit	einen Ansprechpartner, Zeit für Freigaben und Besprechung
Passt gut zu	eigenem Sicherheitsteam oder starker IT	Organisationen ohne eigenes Sicherheitsteam

Drei Fragen für eine erste Richtung

Gibt es bei Ihnen Personen, die sich hauptsächlich um IT-Sicherheit kümmern? Haben diese Personen regelmäßig Zeit, Testergebnisse abzuarbeiten? Ändert sich Ihre IT so oft, dass Sie nach jeder Änderung selbst testen wollen? Wer dreimal mit Ja antwortet, ist mit einer eigenen Lizenz gut bedient. Sonst ist der Managed Service meist der bessere Start.

06

Wie die n-komm unterstützt

Die n-komm GmbH aus Karlsruhe bietet beide Ansätze aus einer Hand. Manuelle Penetrationstests führen ausschließlich eigene Pentester in Deutschland durch, mit fast zehn Jahren Praxis und ohne anonyme Subunternehmer. Wir testen extern und intern einschließlich Active Directory, prüfen Webanwendungen und Schnittstellen, Microsoft 365, Entra ID und Cloud-Umgebungen. Kritische Funde melden wir ohne Verzug, der Bericht enthält eine Zusammenfassung für die Geschäftsleitung und einen technischen Teil. Einen Nachtest können Sie zusätzlich beauftragen.

Für automatisiertes Pentesting setzen wir Pentera ein und sind langjähriger Pentera-Partner. Pentera ist eine Plattform, die echte Angriffstechniken in Ihrer Umgebung nachstellt und die Funde nach ausnutzbaren Angriffswegen priorisiert, im Managed Service ebenso wie mit eigener Lizenz. Wir nutzen das gesamte Portfolio für interne Infrastruktur, externe Angriffsfläche und Cloud. Jeder Test läuft kontrolliert, Umfang, Freigaben und Testfenster stimmen wir vorab mit Ihnen ab.

Im Managed Service planen unsere Experten die Tests, führen sie durch, werten sie aus und besprechen die Ergebnisse persönlich mit Ihnen. Tests, Bericht, Besprechung und Nachtest sind enthalten. Den Rhythmus legen Sie fest, die meisten unserer Kunden testen halbjährlich oder quartalsweise. Das Schließen der Lücken ist nicht Teil des Managed Service: Ihr Team setzt die Empfehlungen um, oder unsere eigenen Techniker übernehmen das auf Wunsch nach gesondertem Angebot.

Der Ablauf im Managed Service ist klar gegliedert: Im Vorgespräch legen wir Umfang und Rhythmus fest, Sie geben Umfang und Testfenster schriftlich frei. Unsere Experten testen kontrolliert, Sie erhalten die Ergebnisse nach Risiko bewertet und besprechen sie mit uns. Im Nachtest prüfen wir gezielt, ob die geschlossenen Lücken wirklich zu sind, und der nächste Test im vereinbarten Rhythmus zeigt, ob neue Lücken entstanden sind. Im Vergleich der Berichte sehen Sie, wie sich Ihre Sicherheitslage entwickelt, und nutzen sie als Nachweis für NIS2, ISO 27001 oder Ihre Versicherung.

Mit einer eigenen Lizenz läuft Pentera On-Premises in Ihrem Rechenzentrum, die Lizenz mieten Sie im Abonnement. Wir richten die Plattform ein, schulen Ihr Team, fahren die ersten Tests gemeinsam und begleiten Sie auf Wunsch im Betrieb. Durch eine besondere Vereinbarung mit Pentera bieten wir eigene Lizenzen auch kleineren Unternehmen an. Ein Wechsel vom Managed Service zur eigenen Lizenz ist möglich, wenn Ihr Team so weit ist.

Weil wir beides anbieten, kombinieren wir manuelle und automatisierte Tests nach Ihrem Bedarf: zum Beispiel einen manuellen Pentest für Webanwendungen und besondere Systeme und Pentera für die wiederkehrende Kontrolle von Netzwerk, Active Directory und Cloud. Im Vorgespräch legen wir gemeinsam fest, welche Bereiche wie geprüft werden, und sprechen ein Restrisiko für den Betrieb offen an.

Die n-komm ist selbst nach ISO/IEC 27001 zertifiziert. Als Familienunternehmen in zweiter Generation begleiten wir Unternehmen und Verwaltungen langfristig. Auf Wunsch zeigen wir Ihnen Pentera in einer Live-Demo.

Aus der Praxis

Ein Landratsamt mit rund 1.500 Endpoints nutzt Pentera als Managed Service von n-komm. Seit dem Start sind 70 % der gefundenen Schwachstellen behoben, an weiteren wird gearbeitet. Die Erfahrung aus dem Projekt: Wer dranbleibt, immer wieder testet und die Lücken schließt, verbessert seine Sicherheit Schritt für Schritt.

Checkliste: Pentest-Strategie festlegen

- [ ] Welche Fragen soll die Prüfung beantworten, und welche Systeme gehören dazu?
- [ ] Wann wurde Ihre IT zuletzt aus Sicht eines Angreifers geprüft, und was hat sich seitdem verändert?
- [ ] Welche Systeme brauchen die Tiefe eines manuellen Tests, etwa Webanwendungen oder besondere Systeme?
- [ ] Welche Bereiche sollen wiederholt automatisiert geprüft werden, etwa Netzwerk, Active Directory und Cloud?
- [ ] Wer darf Tests freigeben, und wer muss vorher informiert werden?
- [ ] Welche Systeme sind so kritisch, dass sie besonders vorsichtig oder gar nicht getestet werden?
- [ ] Wer bewertet die Funde, und wer schließt die Lücken, Ihr Team oder ein Dienstleister?
- [ ] Wie prüfen Sie, ob die Maßnahmen wirken?
- [ ] Hat Ihr Team Zeit und Sicherheitswissen für eine eigene Lizenz, oder passt ein Managed Service besser?
- [ ] Welche Nachweise brauchen Sie für NIS2, ISO 27001, Versicherung oder Kunden?

Ist Ihre IT heute noch so sicher wie beim letzten Test?

Im kostenlosen Erstgespräch klären wir in 30 Minuten, welche Systeme manuell getestet werden sollten und ob automatisiertes Pentesting mit eigener Lizenz oder als Managed Service zu Ihnen passt. Auf Wunsch mit Live-Demo von Pentera. Per Teams oder Telefon, unverbindlich.

Kostenloses Erstgespräch vereinbaren

---

n-komm GmbH · Karlsruhe
Tel. +49 721 35 46 00 · info@n-komm.de
n-komm.de/cyber-security/automatisiertes-pentesting-pentera/

n-komm. Unser IT Partner

Stand November 2026. Dieses Whitepaper gibt einen fachlichen Überblick und ersetzt keine individuelle Beratung. © n-komm GmbH