Kiteworks

# Zertifiziert, geprüft, gehackt:
## Warum Bug-Bounty-Programme den Unterschied machen

April 2026

Florian Scheuer – Director, Product Security, Kiteworks
Nadine Hoogerwerf – Global IT CISO, Kiteworks

# Zusammenfassung

Echte IT-Sicherheit lässt sich weder zertifizieren noch in einem Bericht dokumentieren. Sie entsteht dort, wo ein Produkt kontinuierlich und unter realen Bedingungen auf seine Widerstandsähigkeit geprüft wird – also unter denselben Bedingungen, unter denen auch Angreifer vorgehen.

In den meisten Gesprächen zwischen Unternehmen und ihren Softwarelieferanten über das Thema Sicherheit bleibt man weit hinter diesem Anspruch zurück. Compliance-Zertifizierungen sind wertvoll, aber ihr Prüfungsgegenstand ist die Organisation, nicht das Produkt: Sie belegen, dass ein Unternehmen sicherheitsbewusst aufgestellt ist – nicht, dass seine Software einem gezielten Angriff standhält. Penetrationstests gehen einen Schritt weiter, sind aber strukturell begrenzt: feste Zeitfenster, vorab definierte Prüfumfänge, ein einzelnes Team. Ein Pentest, der am Freitag abgeschlossen wird, sagt nichts über die Schwachstelle aus, die am Montag mit dem nächsten Release in Produktion geht.

Angreifer spielen nach anderen Regeln. Sie sind geduldig, hochspezialisiert und kreativ. Kein Scope-Dokument schränkt sie ein, keine Berichtsfrist treibt sie zur Eile. Sie nehmen sich die Zeit, ein Produkt wirklich zu verstehen – oft über Monate – und verbinden Beobachtungen, die kein zeitlich begrenzter Test jemals hätte zusammenführen können. Sie brauchen nur einen einzigen Weg hinein, und sie haben so lange, wie sie brauchen, um ihn zu finden.

Bug-Bounty-Programme sind das Testmodell, das dieser Realität gerecht wird. Wer sein Produkt einem weltweiten Netzwerk spezialisierter Sicherheitsforscher öffnet und valide Befunde substanziell vergütet, schafft eine kontinuierliche, praxisnahe Überprüfung, die kein punktueller Test leisten kann. Die Forscher bringen tiefes Fachwissen mit, investieren erhebliche Zeit und haben einen klaren finanziellen Anreiz, echte Schwachstellen zu finden – nicht, um einen Bericht zu füllen. Im Laufe der Zeit wird das Produkt auf diese Weise gegen potenzielle Angriffe gehärtet.

Für Sicherheitsverantwortliche ist diese Unterscheidung unmittelbar handlungsrelevant. Compliance-Zertifikate und Pentestberichte gehören weiterhin zur Due Diligence – sie bilden jedoch die Mindestanforderung, nicht das Qualitätsmerkmal. Die entscheidende Frage ist eine andere: Investiert dieser Anbieter in eine kontinuierliche, realitätsnahe Sicherheitsüberprüfung? Betreibt er ein Bug-Bounty-Programm, wie lange läuft es bereits, wie umfassend ist der Prüfumfang – und sind die Prämien hoch genug, um diejenigen Forscher anzuziehen, die wirklich relevante Schwachstellen identifizieren können?

Kiteworks hat genau diese Struktur aufgebaut. Für unser Kernprodukt betreiben wir mehrere Bug-Bounty-Programme – sowohl private als auch öffentliche – auf zwei unabhängigen Plattformen. Für jedes Produkt, das durch eine Akquisition Teil der Kiteworks-Gruppe wird, etablieren wir ein eigenes Programm. Wir lassen uns selbst an diesem Standard messen – denn wenn eines Tages die Frage gestellt wird, nicht ob ein Zertifikat vorlag, sondern ob wirklich alles Mögliche getan wurde, um einen Sicherheitsvorfall zu verhindern, dann zählt nur eine Antwort: eine, die auf allen drei Stufen aufgebaut ist: Governance, technische Validierung und kontinuierliche Sicherheitsüberprüfung.

# Inhaltsverzeichnis



# 1. Die eigentliche Frage

Wenn Unternehmen einen Softwareanbieter evaluieren, hat sich der Penetrationstest als Standardnachweis für Sicherheit etabliert. Anbieter beauftragen Tests, erhalten Berichte und stellen Zusammenfassungen für potenzielle Kunden bereit. Anforderungen werden erfüllt, Checklisten abgehakt. Das Ganze macht einen sehr gründlichen Eindruck – ein Team aus Spezialisten, eine definierte Methodik, ein schriftlicher Bericht mit identifizierten Schwachstellen und Handlungsempfehlungen. Die Frage, die dabei gestellt wird, lautet: Wurden Sie getestet? Die Frage, auf die es wirklich ankommt, lautet: Ist Ihr Produkt sicher? Beides ist nicht dasselbe.

Dabei hat ein Penetrationstest durchaus seinen Wert. Er ist eine legitime und sinnvolle Sicherheitsmaßnahme, und Unternehmen, die regelmäßig Tests durchführen lassen, sind nachweislich sicherheitsbewusster als solche, die darauf verzichten. Das Problem liegt nicht im Penetrationstest an sich, sondern in der Gefahr, sich ausschließlich auf dessen Ergebnisse zu verlassen und die Sicherheit daran zu bemessen.

Software ist nicht statisch, und ein punktueller Bericht kann dieser Realität nicht gerecht werden. Der Code entwickelt sich weiter, Abhängigkeiten ändern sich, neue Funktionen vergrößern die Angriffsfläche, Deployments verändern Konfigurationen auf eine Weise, die kein früherer Test hätte vorhersehen können. Ein Angreifer, der heute das Produkt eines Anbieters ins Visier nimmt, interessiert sich weder für den Umfang noch für den Zeitplan eines Engagements, das vor Monaten abgeschlossen wurde.

Wer dem Bedrohungsgeschehen wirklich einen Schritt voraus sein will, versteht diesen Unterschied. Penetrationstests sind ein wertvoller, aber begrenzter Baustein – und wer es ernst meint mit Sicherheit, investiert darüber hinaus: in kontinuierliche, anreizbasierte Tests, die die Realität von tatsächlichen Angriffen simulieren. Das wichtigste Instrument dafür ist das Bug-Bounty-Programm.

Dieses Whitepaper zeigt auf, was Penetrationstests leisten – und wo ihre strukturellen Grenzen liegen. Es plädiert für Bug-Bounty-Programme nicht als Ersatz für bestehende Sicherheitsmaßnahmen, sondern als die entscheidende Maßnahme, die die Lücke zwischen einem soliden Sicherheitsrahmen und einer wirklich sicheren und widerstandsfähigen operativen Sicherheitsarchitektur schließt. Und es gibt Sicherheitsverantwortlichen konkrete Orientierung bei der Lieferantenauswahl – denn die richtigen Fragen bereits zu Beginn zu stellen, ist selbst eine Sicherheitsentscheidung.

# 2. Compliance und Zertifizierung: Fundament, nicht Ziellinie

Für Unternehmen, die mit sensiblen Daten arbeiten oder kritische Dienste betreiben, ist die Umsetzung eines Compliance-Programms zu Recht essentiell. Rahmenwerke wie ISO 27001, SOC 2 oder die Anforderungen aus NIS2 und DORA existieren, weil die Erfahrung gezeigt hat, dass Unternehmen ohne strukturiertes Sicherheits-Management vorhersehbare und vermeidbare Fehler begehen. Zertifizierungen belegen, dass ein Anbieter die notwendige Grundlagenarbeit geleistet hat: Verantwortlichkeiten sind klar geregelt, Richtlinien dokumentiert, Prozesse für den Umgang mit Sicherheitsvorfällen definiert – und das Unternehmen unterzieht sich regelmäßig einer externen Überprüfung.

Das ist nicht selbstverständlich. Ein Anbieter ohne diese Grundlagen stellt ein Risiko dar, das durch technische Tests allein nicht aufgefangen werden kann. Fehlende oder unklare Governance – unkontrollierte Zugriffsrechte, undokumentierte Systeme, fehlende Notfallpläne – erzeugt Schwachstellen organisatorischer Natur. Compliance-Rahmenwerke sind genau dafür gemacht, solche Lücken zu schließen – und sie tun das effektiv.

Dennoch ist es wichtig, die Grenzen dieser Frameworks klar zu verstehen.

Zertifizierungen beurteilen, ob ein Unternehmen sicherheitsbewusst aufgestellt ist und auch so handelt. Sie prüfen Prozesse, Dokumentation, Organisationsstrukturen und gelebte Sicherheitskultur. Was sie nicht leisten – und strukturell nicht leisten können – ist die Beurteilung, ob die konkrete Software, die dieses Unternehmen entwickelt oder betreibt, ausnutzbare Schwachstellen enthält. Das ist schlicht nicht ihr Prüfungsgegenstand.

Ein Unternehmen kann ISO 27001 zertifiziert sein und gleichzeitig Software ausliefern, die eine kritische Schwachstelle in der Authentifizierung enthält. Es kann ein SOC-2-Audit erfolgreich absolvieren und dabei eine Schnittstelle betreiben, die unter bestimmten Bedingungen sensible Daten preisgibt. Das Zertifikat ist in diesen Fällen nicht falsch – es beantwortet lediglich eine andere Frage als die, die für einen Angreifer relevant ist.

Das ist kein Versagen der Compliance-Rahmenwerke. Es ist ihre natürliche Grenze – und eine, die Sicherheitsverantwortliche klar im Blick haben müssen. Zertifizierungen schaffen das notwendige Fundament. Sie zeigen, dass ein Anbieter Sicherheit als Organisation ernst nimmt. Ob sein Produkt einem gezielten Angriff standhält, ist eine andere Frage – und sie erfordert eine andere Antwort.

# 3. Wert und Grenzen von Penetrationstests

Penetrationstests haben sich in der Sicherheitsbranche etabliert, weil sie genau die Frage zu beantworten scheinen, die Compliance-Frameworks nicht beantworten können. Während eine Zertifizierung die Organisation bewertet, richtet sich ein Penetrationstest auf das Produkt selbst. Ein erfahrenes Team versucht gezielt, Schwachstellen zu identifizieren und auszunutzen, dokumentiert seine Erkenntnisse und liefert einen Bericht mit konkreten Handlungsempfehlungen. Das ist praxisnah, technisch fundiert und produktorientiert.

Der Nutzen ist unbestritten. Ein sorgfältig durchgeführter Penetrationstest deckt Schwachstellen auf, die internen Teams entgangen sind, überprüft das Verhalten von Sicherheitskontrollen unter realen Bedingungen und liefert eine dokumentierte Grundlage für einen strukturierten Behebungsprozess. Für viele Compliance-Frameworks ist ein Penetrationstest zudem eine formale Voraussetzung – und die Ergebnisse, die er liefert, erfüllen diese Anforderung in angemessener Weise.

Die Grenzen des Modells sind jedoch struktureller Natur. Sie spiegeln nicht die Qualität eines bestimmten Unternehmens oder Teams wider – sie sind dem Ansatz selbst inhärent.

**Die erste Einschränkung entsteht durch den Zeitrahmen.** Ein typischer Penetrationstest dauert ein bis vier Wochen. Dieses Zeitfenster klingt ausreichend – bis man bedenkt, was ein erfahrener Sicherheitsforscher leisten muss, bevor er überhaupt mit der eigentlichen Suche nach Schwachstellen beginnen kann. Das Verständnis der Produktarchitektur, die Analyse der Angriffsfläche, die Identifikation von Schnittstellen und Datenflusse – all das erfordert Zeit und muss abgeschlossen sein, bevor die eigentliche Arbeit beginnt. Bei einem zweiwöchigen

Engagement geht ein erheblicher Teil davon für Onboarding, Abstimmung des Scopes und die Erstellung des Abschlussberichts drauf. Das verbleibende Zeitfenster für tiefgehende Tests kann auf wenige Tage schrumpfen. Für ein ausgereiftes, funktionsreiches Produkt reicht das in den seltensten Fällen aus, um über die offensichtlicheren Schwachstellen hinauszugehen.

**Die zweite Einschränkung entsteht durch den verfügbaren Erfahrungsschatz.** Ein Penetrationstest liefert die Perspektive und das Fachwissen des beauftragten Teams. Selbst die besten Unternehmen haben Stärken und blinde Flecken. Der Forscher, der eine subtile Schwachstelle in der Geschäftslogik eines Dateifreigabe-Workflows gefunden hätte, ist möglicherweise nicht Teil des beauftragten Teams. Innerhalb eines festen Engagements gibt es keinen Mechanismus, der das ausgleichen könnte. Das Team, das beauftragt wurde, ist das Team, das testet – und seine blinden Flecken werden zum Risiko des Auftraggebers.

**Die dritte Einschränkung entsteht durch den Prüfumfang.** Penetrationstests arbeiten innerhalb klar definierter Grenzen. Das ist verständlich und oft notwendig – ein unklar definierter Scope schafft operative Risiken und rechtliche Unsicherheiten. Die Konsequenz ist jedoch, dass relevante Teile der tatsächlichen Angriffsfläche möglicherweise ungeprüft bleiben. Angreifer interessieren sich nicht für Scope-Dokumente. Sie untersuchen die Schnittstelle, die aus dem Engagement ausgeschlossen wurde, den Legacy-Endpunkt, der als nicht relevant eingestuft wurde, die Konfiguration, an die niemand gedacht hat. Was außerhalb des vereinbarten Umfangs liegt, erscheint schlicht nicht im Bericht.

**Die vierte Einschränkung entsteht durch die Anreizstruktur.** Penetrationstest-Unternehmen werden für einen definierten Zeitraum beauftragt und nach Aufwand vergütet. Es gibt keinen finanziellen Anreiz, mehr Schwachstellen zu finden oder tiefer in ein Produkt einzudringen – das Engagement endet, wenn die Zeit abgelaufen ist, unabhängig davon, was noch unentdeckt geblieben ist. Das ist keine Kritik an der Professionalität der Tester, sondern eine sachliche Beobachtung darüber, wie dieses Modell funktioniert. Honoriert wird die Lieferung eines Berichts – nicht die Tiefe der Untersuchung.

In der Summe bedeutet das: Ein Penetrationstest liefert – unabhängig davon, wie kompetent er durchgeführt wird – eine begrenzte und zeitlich beschränkte Momentaufnahme der Sicherheitslage eines Produkts. Er ist ein wertvoller Beitrag und eine angemessene Antwort auf bestimmte Compliance-Anforderungen. Aber er ist eben eine Momentaufnahme – aufgenommen durch ein enges Zeitfenster, von einem Team, das das Produkt gerade erst kennenlernt, während die Uhr bereits läuft – und das den Abschlussbericht zu schreiben beginnt, bevor die Erkundung wirklich abgeschlossen ist.

# 4. Das Vorgehen von Angreifern

Um zu verstehen, warum Bug-Bounty-Programme wirksam sind, lohnt ein kurzer Blick auf die Bedrohungsrealität, die sie abbilden sollen – nicht im technischen Detail, sondern im Hinblick auf die grundlegende Asymmetrie im Bereich der Cyber Security.

Ein Angreifer, der ein Softwareprodukt ins Visier nimmt, arbeitet unter völlig anderen Bedingungen als ein Penetrationstester. Es gibt keinen vereinbarten Scope, kein Zeitlimit, keine Anforderung, Ergebnisse in einem strukturierten Bericht festzuhalten. Kein Onboarding, kein Kick-off. Der Angreifer fängt einfach an – und hört erst auf, wenn das Ziel uninteressant wird oder der Aufwand den möglichen Gewinn nicht mehr rechtfertigt.

Geduld ist dabei der am häufigsten unterschätzte Faktor. Während ein Penetrationstest in Wochen gemessen wird, kann ein motivierter Angreifer Monate damit verbringen, ein Produkt wirklich zu durchdringen, bevor er einen konkreten Angriff startet. Er liest Dokumentation, testet Randfälle, beobachtet das Verhalten der Anwendung unter ungewöhnlichen Bedingungen und entwickelt ein immer detaillierteres Bild des Systems. Die Schwachstelle, die er schließlich ausnutzt, wird oft erst nach dieser langen Beobachtungsphase sichtbar – etwas, das kein zeitlich begrenztes Engagement hätte aufdecken können.

Spezialisierung ist der zweite entscheidende Faktor. Angreifer sind keine homogene Gruppe, die nach einem einheitlichen Schema vorgeht. Es handelt sich um ein vielfältiges Netzwerk hochspezialisierter Einzelpersonen – jemand, der seit Jahren Authentifizierungsprotokolle analysiert, jemand anderes, der sich ausschließlich mit Schwachstellen in der Dateiverarbeitung beschäftigt, ein Dritter, der die spezifischen Eigenheiten eines bestimmten

Frameworks in- und auswendig kennt. Jedes Produkt zieht früher oder später die Aufmerksamkeit von jemandem auf sich, dessen Expertise zufällig genau auf seine verwundbarsten Stellen trifft. Kein fest zusammengestelltes Team kann diese Bandbreite an Spezialwissen abbilden.

Kreativität ist der dritte Faktor. Wirklich schwerwiegende Schwachstellen werden äußerst selten durch das Abarbeiten von Checklisten identifiziert. Häufig entstehen sie aus einer Kombination von Schwachstellen: ein Fehler in einer Komponente, der erst dann kritisch wird, wenn er mit einer Unsauberkeit einer anderen verknüpft wird; eine Designannahme, die in allen bekannten Szenarien funktioniert, aber unter einer bestimmten Abfolge von Aktionen versagt, auf die niemand gekommen wäre. Solche Entdeckungen erfordern nicht nur technisches Können, sondern echte Neugier und die Bereitschaft, ungewöhnlichen Spuren zu folgen – das Ergebnis tiefer Vertrautheit mit einem Ziel, nicht einer strukturierten Methodik unter Zeitdruck.

Die Schlussfolgerung für das Security Testing ist eindeutig: Wer die wirklich bedrohlichen Schwachstellen identifizieren möchte, benötigt ein Testmodell, das widerspiegelt, wie Angreifer tatsächlich vorgehen. Geduldig, spezialisiert, kreativ und ohne künstliche Einschränkungen. Dieses Modell findet in einem Bug-Bounty-Programm eine wesentlich bessere Entsprechung als in einem Penetrationstest.

# 5. Bug-Bounty-Programme: Kontinuierliche Sicherheit in der Praxis

Ein Bug-Bounty-Programm ist im Kern eine Einladung. Der Anbieter öffnet sein Produkt für die Überprüfung durch ein weltweites Netzwerk von Sicherheitsexperten und verpflichtet sich, valide und relevante Schwachstellen substanziell zu vergüten. Die Hacker entscheiden selbst, ob sie teilnehmen – auf Basis ihres Interesses, ihrer Expertise und der Einschätzung, ob ihre Fähigkeiten zum Ziel passen. Es gibt kein fixes Enddatum, keine vorab verhandelte Scope-Begrenzung und kein vorgegebenes Team.

Genau dieser strukturelle Unterschied zum Penetrationstest erklärt, warum Bug-Bounty-Programme eine grundlegend andere Wirkung erzielen.

**Kontinuierliche Abdeckung statt punktueller Momentaufnahme.** Ein Bug-Bounty-Programm läuft parallel zur Produktentwicklung. Neue Features fallen automatisch in den Scope. Aktualisierte Abhängigkeiten können sofort untersucht werden. Ändert sich eine Konfiguration, bemerken erfahrene Hacker, die das Produkt bereits gut kennen, wenn sich etwas anders verhält als erwartet. Das Assessment muss nicht neu aufgesetzt werden, wenn sich der Code weiterentwickelt – es läuft einfach weiter und spiegelt den aktuellen Stand des Produkts wider.

**Zugang zu einem breiten Erfahrungsschatz statt eines fixen Teams.** Anstelle der Fähigkeiten einer einzelnen beauftragten Firma zieht ein Bug-Bounty-Programm Hacker aus aller Welt mit unterschiedlichsten Spezialisierungen an. Wer eine kritische Schwachstelle in einem Produkt findet, ist häufig jemand, der seit Jahren genau die Klasse von Schwachstellen untersucht, für die diese spezifische Architektur anfällig ist. Diese Passung zwischen Spezialwissen und konkreter Schwachstelle lässt sich in einem festen Engagement nicht herbeiführen – sie entsteht natürlich aus der Dynamik eines offenen Programms.

**Tiefes Produktverständnis als Grundlage für qualitativ hochwertige Ergebnisse.** Hacker im Rahmen eines Bug-Bounty-Programms sind nicht auf ein zweiwöchiges Zeitfenster beschränkt. Wer ein Programm als lohnend einschätzt, kann Wochen oder Monate damit verbringen, das Produkt zu durchdringen, bevor die erste Schwachstelle gemeldet wird. Dieses akkumulierte Verständnis ist die Voraussetzung für die Entdeckung komplexer, verketteter Schwachstellen – solcher, die nur durch die Verknüpfung von Beobachtungen aus verschiedenen Bereichen des Produkts sichtbar werden. Genau diese Schwachstellen bleiben bei zeitlich begrenzten Engagements häufig unentdeckt – und genau sie stellen in der Praxis das größte Risiko dar.

**Finanzielle Anreize sichern die Qualität der Ergebnisse – aber nur, wenn diese ausreichend attraktiv sind.** Hacker werden für valide Schwachstellen vergütet, nicht für aufgewendete Zeit. Es gibt keinen Grund, einen Bericht mit Schwachstellen geringer Relevanz aufzufüllen, und keinen Grund, die Suche zu beenden, wenn eine Frist naht. Wer vermutet, dass in einem bestimmten Bereich des Produkts etwas Bedeutsames steckt, wird weitersuchen – weil

die Vergütung für eine kritische Schwachstelle üblicherweise überproportional attraktiv ist. Das Programm honoriert Ergebnisse, nicht Aufwand.

Diese Dynamik funktioniert jedoch nur, wenn substanzielle Beträge ausgeschüttet werden. Erfahrene Hacker haben die Wahl. Sie entscheiden, wo sie ihre Zeit investieren – und wählen Programme, die ihre Arbeit angemessen vergüten. Ein Programm, das lediglich symbolische Preise verteilt, darf keinen ernstzunehmenden Einsatz erwarten. Ein Programm, das wettbewerbsfähig vergütet und damit signalisiert, dass der Anbieter externe Überprüfung wirklich schätzt, zieht diejenigen Hacker an, die wirklich relevante Schwachstellen identifizieren können. Die Höhe der Vergütung ist kein Kostenposten, der minimiert werden sollte – sie ist der entscheidende Hebel für die Qualität der Ergebnisse.

**Langfristige Wirkung: Das Produkt wird mit der Zeit sicherer.** Das ist möglicherweise der bedeutsamste Vorteil für Kunden, die die Sicherheitsverpflichtung eines Anbieters bewerten möchten. Mit jeder gemeldeten und behobenen Schwachstelle steigt die Widerstandsähigkeit des Produkts. Systemische Schwächen – Architekturmuster, die immer wieder Schwachstellen erzeugen, problematische Abhängigkeiten, wiederkehrende Mängel im Authentifizierungsdesign – werden durch die Häufung der Meldungen erkennbar und können grundlegend behoben werden, anstatt nur symptomatisch. Ein Anbieter, der seit mehreren Jahren ein ernsthaftes Bug-Bounty-Programm betreibt, arbeitet mit einem Produkt, das durch diesen Prozess kontinuierlich gehärtet wurde. Das ist ein qualitativ anderes Sicherheitsniveau als eines, das durch punktuelle Tests aufrechterhalten wird.

Für Kunden hat dies eine sehr fundamentale Bedeutung: Die Wahrscheinlichkeit, Opfer eines Sicherheitsvorfalls zu werden, der durch den eigenen Testprozess des Anbieters hätte verhindert werden können, ist nachweislich geringer. Kein Sicherheitsprogramm eliminiert Risiken vollständig – aber ein gut geführtes Bug-Bounty-Programm reduziert sie messbar. Und in einer Bedrohungslandschaft, in der die Frage nicht lautet, ob Angriffe versucht werden, sondern ob sie erfolgreich sind, ist genau das der Maßstab, an dem Sicherheitsinvestitionen gemessen werden sollten.

# 6. Die drei Stufen zu echter Sicherheit

Die Erkenntnis aus den vorangegangenen Abschnitten lautet nicht, dass die Umsetzung eines Compliance-Frameworks falsch oder Penetrationstests wertlos sind. Sie macht lediglich deutlich, dass Sicherheit kein eindimensionales Konzept ist: Für einen umfassenden Ansatz sind unterschiedliche Stufen erforderlich – und jede dieser Stufen löst ein anderes Problem. Es ist ein grundsätzlicher Fehler davon auszugehen, eine dieser Stufen überspringen oder auf sie verzichten zu können.

Die drei Stufen lassen sich wie folgt beschreiben.

**Stufe 1 – Governance und Prozesse.** Das ist das Fundament, das Compliance-Frameworks und Zertifizierungen aufbauen und überprüfen. Es beantwortet die Frage: Ist dieses Unternehmen sicherheitsbewusst aufgestellt und handelt es auch so? Klare Verantwortlichkeiten, dokumentierte Richtlinien, definierte Prozesse für den Umgang mit Sicherheitsvorfällen, regelmäßige Schulungen, externe Audits – das sind die Bausteine eines umfassenden Schwachstellenmanagements. Dies ist das Fundament für alles Weitere. Ein technisch noch so ausgereiftes Sicherheitsprogramm, das auf dysfunktionaler Governance aufsetzt, wird ein Unternehmen nicht vor den vorhersehbaren Fehlern bewahren, die solide Prozesse verhindern sollen. Diese Stufe ist unverzichtbar – und es ist vollkommen angemessen, von Lieferanten entsprechende Nachweise einzufordern.

**Stufe 2 – Punktuelle technische Validierung.** Das ist die Stufe, auf der Penetrationstests angesiedelt sind. Sie beantwortet die Frage: Hat ein qualifiziertes Team ausnutzbare Schwachstellen identifiziert, als es dieses Produkt unter definierten Bedingungen untersucht hat? Sie liefert technische Tiefe, die Governance-Bewertungen nicht bieten können – konkrete Schwachstellen, reale Angriffspfade, umsetzbare Handlungsempfehlungen. Für viele Compliance-Frameworks ist sie zudem eine formale Voraussetzung, die sie in angemessener Weise erfüllt. Die zuvor beschriebenen Einschränkungen negieren ihren Wert nicht – sie definieren ihren Geltungsbereich. Ein Penetrationstest ist ein wertvoller und notwendiger Beitrag, aber kein vollständiges Bild der Sicherheitslage eines Produkts.

**Stufe 3 – Kontinuierliche Sicherheitsüberprüfung.** Das ist die Stufe, auf der Bug-Bounty-Programme angesiedelt sind – und die Stufe, die die meisten Unternehmen und Anbieter noch nicht vollständig etabliert haben. Sie

beantwortet die Frage: Hält dieses Produkt der Aufmerksamkeit qualifizierter, motivierter und hochspezialisierter Hacker stand, die ohne künstliche Einschränkungen arbeiten? Sie bildet die Bedingungen ab, unter denen echte Angriffe stattfinden. Sie läuft kontinuierlich, passt sich der Produktentwicklung an und liefert Ergebnisse, die die anderen beiden Stufen strukturell nicht erbringen können. Sie ersetzt Stufe 1 und Stufe 2 nicht – sie setzt sie voraus. Aber ohne sie bleibt das Sicherheitsbild fundamental unvollständig.

Die meisten Unternehmen haben Stufe 1 etabliert. Viele haben Stufe 2 in irgendeiner Form. Nur wenige haben ernsthaft in Stufe 3 investiert – und genau in dieser Lücke siedelt sich das Restrisiko an, das letztlich zu Sicherheitsvorfällen führt.

Die praktische Konsequenz ist klar. Bei der Bewertung der Sicherheitslage eines Anbieters sollten Nachweise der Stufen 1 und 2 als Mindestanforderung gelten, nicht als Qualitätsmerkmal. Die entscheidende Frage – diejenige, die einen wirklich sicherheitsverpflichteten Anbieter von einem unterscheidet, der lediglich den Anschein wahrt – ist, ob Stufe 3 vorhanden ist, wie ernsthaft sie ausgestattet ist und wie lange sie bereits läuft.

Ein Anbieter, der diese Frage konkret und transparent beantworten kann, hat eine Verpflichtung übernommen, die über das Bestehen eines Audits hinausgeht – nämlich die kontinuierliche Auseinandersetzung seines Produkts mit der Überprüfung, der es in der Realität standhalten muss.

# 7. Was Sie von Ihrem Anbieter erwarten sollten

Sicherheit ist letztlich auch eine Frage der Lieferkette. Die eigenen Richtlinien, implementierten Kontrollen und erworbenen Zertifizierungen schützen ein Unternehmen nicht vor Schwachstellen in den Produkten, auf die es angewiesen ist. Das Sicherheitsniveau ihres Anbieters determiniert ihr eigenes Sicherheitsniveau – unabhängig davon, ob der Beschaffungsprozess das bereits berücksichtigt.

Das ist die praktische Konsequenz aus allem bisher Dargelegten. Sie weist auf eine konkrete Veränderung in der Art hin, wie Lieferantensicherheit bewertet werden sollte.

Penetrationstestberichte und Compliance-Zertifikate sollten weiterhin Teil der Due Diligence sein – sie enthalten wertvolle Erkenntnisse, und ein Anbieter, der sie nicht vorweisen kann, hat die Mindestanforderungen nicht erfüllt. Aber wer dabei stehen bleibt, akzeptiert eine Sicherheitsbewertung, die genau dort endet, wo die eigentlich entscheidende Frage beginnt.

Die zusätzlichen Fragen, die gestellt werden sollten – und auf deren Antworten es wirklich ankommt – sind folgende:

**Betreiben Sie ein Bug-Bounty-Programm?** Bereits die Antwort auf diese Frage ist aussagekräftig. Ein Anbieter mit einem aktiven Programm hat sich öffentlich zur kontinuierlichen Überprüfung seines Produkts verpflichtet. Ein Anbieter ohne ein solches Programm nicht.

**Ist das Programm öffentlich oder privat?** Öffentliche Programme stehen jedem qualifizierten Hacker offen. Private Programme beschränken die Teilnahme auf einen eingeladenen Kreis. Beide haben ihre Daseinsberechtigung – aber ein öffentliches Programm steht für ein höheres Maß an Offenheit und Überzeugung von der Qualität des eigenen Produkts.

**Wie lange läuft das Programm bereits?** Kontinuität zählt. Ein Programm, das seit mehreren Jahren läuft, hat kumulative Sicherheitsverbesserungen erzielt, die ein kürzlich gestartetes noch nicht liefern konnte. Die Laufzeit ist ein verlässlicher Indikator für die Tiefe der Überprüfung, der das Produkt bereits unterzogen wurde.

**Was deckt der Scope ab?** Ein Programm, das große Teile der tatsächlichen Angriffsfläche ausschließt, bietet eine schwächere Sicherheitsgarantie als eines mit umfassender Abdeckung. Zu verstehen, was im Scope enthalten ist und was nicht, verrät, wo das Vertrauen – und die Zurückhaltung – des Anbieters tatsächlich liegt.

**Sind die Vergütungen attraktiv genug?** Ein Programm existiert auch dann lediglich auf dem Papier, wenn die Prämien zu niedrig angesetzt sind, um ernsthafte Hacker anzuziehen. Wer nach den Vergütungsbereichen fragt – insbesondere für Schwachstellen hoher und kritischer Schwere – erhält ein klares Signal darüber, wie ernst der Anbieter externe Überprüfung wirklich nimmt. Ein Programm, das lediglich symbolische Preise verteilt, darf keinen ernstzunehmenden Einsatz erwarten.

**Wie fließen die Ergebnisse in den Entwicklungsprozess ein?** Der Wert eines Bug-Bounty-Programms liegt nicht allein in den gefundenen Schwachstellen – sondern darin, was mit ihnen geschieht. Ein Anbieter, der einen klaren und schnellen Weg von der Meldung über die Behebung bis zur Auslieferung beschreiben kann, hat das Programm wirklich in seine Sicherheitspraxis integriert – und betreibt es nicht als Marketinginstrument.

Ein Anbieter, der diese Fragen konkret und transparent beantworten kann, beweist etwas, das kein Zertifikat vermitteln kann: dass er sein Produkt an einem Maßstab misst, der nicht von Prüfern definiert wird – sondern von der Realität, der seine Kunden täglich ausgesetzt sind.

Das ist ein echter Unterschied. Und in einer Welt, in der Sicherheitsvorfälle weiterhin auch bei Unternehmen mit lückenlosen Compliance-Portfolios auftreten, ist es möglicherweise die wichtigste Sicherheitsfrage, die ein Einkäufer stellen kann.

# 8. Das Sicherheitsversprechen von Kiteworks

Bei Kiteworks war die Entscheidung, ernsthaft in Bug-Bounty-Programme zu investieren, weder eine Reaktion auf eine Audit-Anforderung noch auf einen Kundenwunsch. Sie war die Konsequenz aus einer einfachen Erkenntnis: Die Maßstäbe, die wir in diesem Whitepaper beschreiben und die wir Ihnen empfehlen, an Ihre Lieferanten anzulegen, müssen zuerst für uns selbst gelten.

Unser Engagement geht weit über ein einzelnes Programm hinaus. Für das Kernprodukt von Kiteworks betreiben wir mehrere Bug-Bounty-Programme – sowohl private als auch öffentliche – auf zwei unabhängigen Plattformen. Diese Struktur ist bewusst gewählt: Private Programme ermöglichen die gezielte Zusammenarbeit mit einem ausgewählten Kreis erfahrener Hacker in sensiblen oder komplexen Produktbereichen, während das öffentliche Programm die zentrale Angriffsfläche einem deutlich breiteren Teilnehmerkreis zugänglich macht. Der parallele Betrieb auf zwei getrennten Plattformen diversifiziert den Pool weiter und reduziert das Risiko, dass blinde Flecken einer einzelnen Plattform oder Community unentdeckt bleiben.

Dieses Engagement endet nicht beim Kernprodukt. Jedes Produkt, das im Rahmen einer Akquisition Teil der Kiteworks-Gruppe wird, erhält ein eigenes Bug-Bounty-Programm – das ist ein Standard, den wir konsequent umsetzen. Für Kunden von Unternehmen, die zur Kiteworks-Familie stoßen, bedeutet das eine unmittelbare und spürbare Verbesserung ihres Sicherheitsniveaus: In nahezu allen Fällen verfügten die übernommenen Produkte vor der Akquisition über kein Bug-Bounty-Programm. Die Einrichtung eines solchen gehört zu den ersten Sicherheitsinvestitionen, die wir nach einer Übernahme vornehmen. Das ist ein konkretes Signal dafür, wie ernst Kiteworks seine Verantwortung gegenüber den Kunden nimmt, die es übernimmt – und ein Beleg dafür, dass eine Akquisition durch Kiteworks für diese Kunden ein höheres Sicherheitsniveau bedeutet, nicht ein niedrigeres.

Die Vergütungsstruktur jedes Programms ist darauf ausgelegt, diejenigen Hacker anzuziehen und zu halten, die wirklich relevante Schwachstellen identifizieren können. Meldungen behandeln wir nicht als isolierte Berichte, die abgehakt werden – sondern als operative Erkenntnisse: Identifizierte Schwachstellen treiben die Behebung voran, deren Ergebnisse fließen in die Weiterentwicklung der Architektur ein, und das kumulative Resultat ist ein Produktportfolio, das kontinuierlich unter realen Bedingungen getestet und gehärtet wird.

Dies kann in der sich schnell entwickelnden Welt der Software nie vollständig ausgeschlossen werden – aber wir haben die Strukturen aufgebaut, die es am wahrscheinlichsten machen, Schwachstellen zu finden, bevor ein Angreifer es tut, und schnell und transparent darauf zu reagieren, wenn sie identifiziert werden.

Für unsere Kunden bedeutet das etwas Konkretes: Produkte, die kontinuierlich überprüft und verbessert werden – gemessen nicht an dem, was Compliance vorschreibt, sondern an dem, was echte Sicherheit erfordert.

# 9. Fazit

Die Sicherheitslandschaft hat sich im vergangenen Jahrzehnt grundlegend weiterentwickelt. Compliance-Frameworks sind strenger geworden, Penetrationstests gehören zum Standard, und das Bewusstsein für Cyberrisiken war in Unternehmen nie größer. Das ist ein echter Fortschritt.

Doch die Bedrohungslandschaft hat sich parallel dazu weiterentwickelt. Angreifer sind geduldiger, spezialisierter und kreativer als je zuvor – und sie nutzen genau die Lücken, die strukturell begrenzte Testmodelle hinterlassen. Die Distanz zwischen dem, was Compliance leistet, und dem, was echte Sicherheit erfordert, hat sich nicht verringert. In vielen Bereichen hat sie sich vergrößert.

Die Kernthese dieses Whitepapers ist nicht kompliziert. Governance und Zertifizierung belegen, dass ein Unternehmen Sicherheit ernst nimmt. Penetrationstests liefern eine wertvolle, aber zeitlich und inhaltlich begrenzte Bestandsaufnahme der Schwachstellen eines Produkts. Bug-Bounty-Programme leisten das, was keines von beiden kann: eine kontinuierliche, realitätsnahe Überprüfung durch ein weltweites Netzwerk spezialisierter Hacker, die den finanziellen Anreiz haben, zu finden, was anderen entgeht – und die Zeit, es tatsächlich zu tun.

Jede der drei beschriebenen Stufen eines professionellen Schwachstellenmanagements hat ihre Berechtigung. Keine ersetzt die andere. Aber die Stufe, die am direktesten darüber entscheidet, ob ein versierter Angreifer eine ausnutzbare Schwachstelle findet, bevor es der Anbieter tut – das ist die Stufe, die in den meisten Gesprächen über Lieferantensicherheit noch immer nicht erreicht wird.

Für Sicherheitsverantwortliche, die Anbieter evaluieren, ist die Botschaft klar: Bestehen Sie auf der Umsetzung der organisatorischen Basis, aber setzen Sie die Messlatte höher. Zertifikate und Penetrationstestberichte sind der Anfang eines verantwortungsvollen Gesprächs über Cyber-Sicherheit – nicht sein Abschluss. Die Anbieter, die dem Bedrohungsgeschehen wirklich voraus sind, haben zusätzliche Maßnahmen umgesetzt: Sie haben ihre Produkte einer kontinuierlichen Überprüfung geöffnet, in deren Qualität investiert und die internen Prozesse aufgebaut, um aus den Ergebnissen zu lernen und zu handeln.

Wenn die Frage eines Tages nicht mehr lautet, ob ein Zertifikat vorlag, sondern ob wirklich alles Mögliche getan wurde, um einen Sicherheitsvorfall zu verhindern – und diese Frage wird gestellt werden – dann zählt nur, ob alle drei Stufen des Schwachstellenmanagements etabliert wurden. Nicht nur die, die einen Prüfer zufriedenstellen. Alle drei.