AUSGABE 3

DEN WERT VON SICHERHEIT IN EINEM UNSICHEREN UMFELD BEWERTEN

VERTRAUENSBERICHT 2020

Synack

Vertrauen ist von entscheidender Bedeutung.

Großflächige Bereitstellung von intelligenten Penetrationstests. Die Plattform von Synack greift auf die weltweit talentiertesten ethischen Hacker zurück und nutzt maschinelle Intelligenz, um unterbrechungsfreie Abdeckung zu realisieren und umsetzbare Ergebnisse zu liefern.

Wir sind Synack: die vertrauenswürdigste Crowdsourcing-basierte Sicherheitsplattform der Welt.

Synack

Inhalt

FRAGEN VON C-LEVEL-MANAGERN:

„Wie kann ich die digitale Transformation meines Unternehmens beschleunigen und sicherstellen, dass diese neuen digitalen Systeme sicher sind?“ „Kann ich darauf vertrauen, dass mein Unternehmen unter dem Druck einer schnellen Bereitstellung den Aspekt Cybersicherheit in unseren Systemen auch angemessen berücksichtigt?“ „Wie kann ich sicher sein, dass Anwendungen, die in der schnellen fortlaufenden Entwicklung von Agile DevOps konzipiert werden, sicher sind?“ „Wie sicher sind meine Systeme und Anwendungen im Vergleich zu denen von Mitbewerbern und zu anderen Branchen?“ „Kann der Vorstand darauf vertrauen, dass die digitale Transformation, die sie mir übertragen haben, sicher ist und dass der Name unseres Unternehmens nicht irgendwann in den Schlagzeilen der Tagespresse erscheint?“

Die Cybersicherheit der digitalen Assets Ihres Unternehmens ist genauso wichtig wie unsere körperliche Gesundheit. 98 % der amerikanischen Staatsbürger haben sich nicht mit COVID-19 infiziert. Wenn Sie aber zu den 2 % gehören, die sich angesteckt haben, dann haben sie gelitten. 97 % der mit COVID-19 infizierten US-Bürger haben sich mittlerweile wieder völlig erholt, für 3 % gilt das nicht. Die Wahrscheinlichkeit, mit der Ihr Unternehmen schwere Schäden aufgrund eines Cyberangriffs erleidet, ist gering. Trifft es Sie aber doch, dann können die Auswirkungen verheerend sein. Viele Menschen achten auf Ihre Gesundheit und nehmen jährliche Vorsorgeuntersuchungen wahr. Und dabei werden auch häufig Probleme erkannt, die wir korrigieren, bevor sie sich zu einem ernsten Gesundheitsproblem entwickeln. In meinem Fall entdeckten die Ärzte bei einem Belastungs-EKG eine zu 90 % verstopfte Koronararterie. Glücklicherweise bin ich nun stolzer Träger eines Stents und bin nicht in die Statistik der Herzinfarkte eingegangen.

In der aktuellen COVID-19-Pandemie hat sich gezeigt, dass durch Testen Hunderttausende Leben gerettet werden konnten.

ICH BIN SCHON SEIT ÜBER 30 JAHREN IM BEREICH CYBERSICHERHEIT TÄTIG UND KANN IHNEN VERSICHERN, DASS DURCH PENETRATIONSTESTS SCHWACHSTELLEN ENTDECKT WURDEN, DIE – WÄREN SIE NICHT BEHOBEN WORDEN – ZEHNTAUSENDE UNTERNEHMEN ZU ANGRIFFSZIELEN GEMACHT HÄTTEN, MIT GRAVIERENDEN FOLGEN: GESCHÄFTSUNTERBRECHUNGEN, VERLUST VON GEISTIGEM EIGENTUM, SAMMELKLAGEN, NEGATIVSCHLAGZEILEN IN DER PRESSE UND SCHLIMMERES.

UM „CYBER-GESUNDHEIT“ FÜR IHRE DIGITALEN ASSETS ZU GEWÄHRLEISTEN, IST DER PENETRATIONSTEST IST DER ULTIMATIVE STRESSTEST.

Standardscanner, die auf Schwachstellen prüfen, sind hilfreich, um einige häufige und nicht besonders kritische Schwachstellen zu finden. Intelligente Penetrationstests können allerdings diese zu „90% verstopften Arterien“ finden, die den Tod bringen könnten. Im Vertrauensbericht 2020 von Synack wird klar, dass die Unternehmen, die die ungebrochene Flut an Cyberangriffen überleben, zu den Unternehmen gehören, die regelmäßig möglichst viele ihrer digitalen Assets testen, und zwar mit einem Detailgrad, der an die Kritikalität der einzelnen Assets angepasst ist.

Irgendwie ist das doch Ironie: Die digitalen Technologien, die wir nutzen, um unser Unternehmen weiterzubringen, unsere Kosten zu reduzieren, Umsätze und Gewinne zu steigern und Beschäftigung zu fördern, vergrößern gleichzeitig unsere Angriffsfläche für Cyberattacken. In den Umgebungen von heute implementieren wir Agile DevOps mit neuen Softwareversionen, die alle paar Wochen bereitgestellt werden. Mit anderen Worten, die Tests, die wir letzten Monat durchgeführt haben, wiesen eine andere Angriffsfläche auf, und damit sind der Test und die Maßnahmen zur Behebung aus dem letzten Monat nicht mehr ausreichend. Wie kann ich darauf vertrauen, dass mit dem System in diesem Monat keine neuen Schwachstellen eingeführt wurden, die die Cybersicherheit bedrohen?

Synack bietet eine etablierte und bewährte marktführende Plattform für intelligente Penetrationstests, die Tausende weltweit bekannte Unternehmen einsetzen, um Schwachstellen in ihren digitalen Assets zu entdecken, die andere nicht finden können. Auf diese Weise können sie die Schwachstellen beheben und teils auch Risiken beseitigen. Hinter den Kulissen bringt Synack die auf Herz und Nieren geprüften hochqualifizierten und erfahrensten Experten aus aller Welt zusammen.

Der Ansatz von Synack für Penetrationstests gilt als wirklich bahnbrechend und bietet sowohl skalierbare als auch fortlaufende Tests von digitalen Assets, wenn neuer Code dafür bereitgestellt wird. Die Plattform vereint Suchergebnisse, die automatische Scans besonders zuverlässig finden können, mit einer Prüfung durch Experten, um die Schwachstellen zu bestätigen, und Sicherheitsexperten, die ihre Kompetenzen und Erfahrung einbringen, um weitere kritische Schwachstellen zu bestimmen, die automatisierten Scans verborgen bleiben. Da alle entdeckten Schwachstellen vollständig geprüft, von Experten bestätigt und umfassend in einem umsetzbaren Schwachstellenbericht beschrieben werden, kommen falsche positive Ergebnisse nur sehr selten vor, und die Behebung geht wesentlich schneller und effizienter vonstatten.

Dieser Ansatz bringt erhebliche Vorteile: Als Erstes wird nach Schwachstellen gesucht, die im Laufe der Zeit entstanden sind, durch Änderungen im Produktionssystem oder durch versehentliche Fehlkonfigurationen. Als Zweites erhalten Sie durch die Vielfalt der Sicherheitsexperten, die sich an den Penetrationstests beteiligen, einen wesentlich umfangreicheren Überblick über Ihre Schwachstellen. Das ist so, als wenn ein Kardiologe, ein Hämatologe und ein Neurologe gemeinsam nach der Ursache einer Erkrankung suchen. Und zu guter Letzt bietet die Synack-Plattform eine pragmatische Analyse wie einfach oder schwer es für einen Cyberangreifer ist, in Ihre kritischen Systeme einzudringen und welche Art von Schaden auftreten könnte, wenn der Angreifer erfolgreich ist.

Synack nennt diese messbare Analyse Attacker Resistance Score (ARS)™, eine Kennzahl zur Messung der Widerstandsfähigkeit.
ARS hilft dem C-Level-Management, zu bestimmen, wie sicher die eigenen Assets im Vergleich zu anderen Unternehmen in der Branche und zu Mitbewerbern sowie zu anderen Branchen sind. Damit lässt sich eine realistische Einschätzung des eigenen Sicherheitsrisikos vornehmen.
Sprich, wenn die ARS angibt, dass Ihre Assets angreifbar sind, selbst durch ein einfachstes Skript in kürzester Zeit, empfiehlt es sich, massiv in Sicherheitsmaßnahmen zu investieren.
Gibt die ARS an, dass Ihr Sicherheitsstatus durchaus mit dem von Fort Knox vergleichbar ist, dann können Sie darauf vertrauen, dass Sie durch die bestehenden Sicherheitsinvestitionen und -maßnahmen abgesichert sind.

DER VERTRAUENSBERICHT 2020 VON SYNACK – EIN MUSS FÜR ALLE, DIE FOLGENDE FRAGEN VOM C-LEVEL-MANAGEMENT, DEM CEO ODER DEM VORSTAND SCHON EINMAL GEHÖRT HABEN: „KANN ICH AUF UNSERE DIGITALEN SYSTEME VERTRAUEN? UND WIE STEHEN WIR IM VERGLEICH ZU ANDEREN UNTERNEHMEN DA?“ ZWEI DER ZEHN HÄUFIGSTEN FRAGEN, DIE ICH IN HUNDERTEN UNTERNEHMEN HÖRE.

MICHAEL CODEN
GLOBAL LEADER CYBERSECURITY PRACTICE, BCG PLATINION
BOSTON CONSULTING GROUP

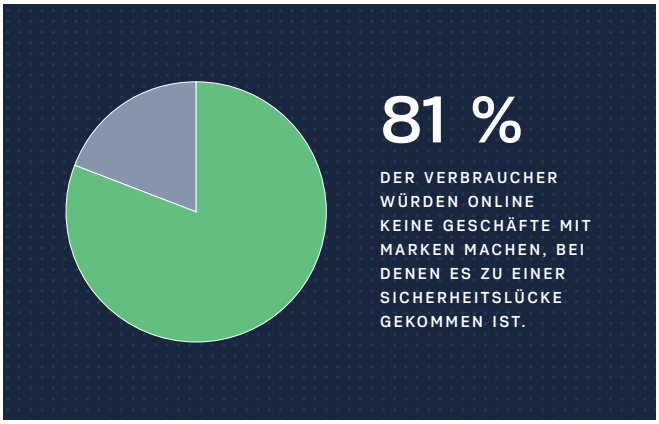
TIEL 1

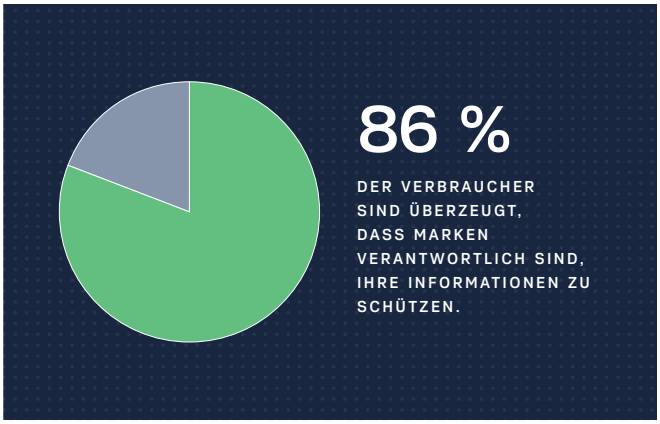
MESSUNGEN

Synack

Vertrauen ist heute wichtiger denn je.

2020 ist ein Jahr, in dem wir ganz neue Herausforderungen in unserer Gesellschaft, der Weltwirtschaft und der Umwelt meistern müssen, während Verbraucher inmitten eines unsicheren Umfelds von ihren liebsten Marken erwarten, positive Veränderungen voranzutreiben, Stabilität und Sicherheit zu bieten und innovative Lösungen zu entwickeln, um die Grundlage für mehr Stabilität in der Gesellschaft und eine gerechtere Zukunft zu legen.





70 % DER VERBRAUCHER GLAUBEN, DASS VERTRAUEN WICHTIGER IST DENN JE,
laut dem Edelman-Bericht „Trust Barometer Special Report: Brand Trust in 2020“. Vertrauen spielt überall eine Rolle, von großen Investitionsentscheidungen bis hin zu alltäglichen Kaufentscheidungen. Wenn Familien über eine mobile App Pizza bestellen, vertrauen sie darauf, dass ihr Lieblingslieferdienst ihre personenbezogenen und Finanzdaten schützt und außerdem frische heiße Pizza pünktlich liefert.

MISSTRAUEN VERBREITET SICH SCHNELL.
Besonders schnell infolge einer Datenschutzverletzung. 81 % der Verbraucher geben an, sie würden mit Marken online nach einer Datenschutzverletzung keine Geschäfte mehr tätigen. Die Consumer Intelligence Series von PwC kommt zu dem Schluss, dass 86 % der Verbraucher glauben, dass Marken dafür verantwortlich seien, ihre Informationen zu schützen. Aber es ist nicht nur das Vertrauen der Verbraucher ausschlaggebend.

LEIDER SIND DATENSCHUTZVERSTÖSSE IMMER NOCH EIN HÄUFIGES PROBLEM.
Das Blutvergießen infolge eines Verstoßes macht häufig umfangreiche und kostenintensive Sanierungen erforderlich. Die Kosten für die massiven Datenschutzverletzungen bei British Airways und Marriott lagen über 100 Millionen US-Dollar. Führungskräfte, die Datenschutzverstöße nicht gut handeln, verlieren häufig ihren Job und müssen mit Strafanzeigen rechnen. Doch es geht nicht nur um Datenschutzverstöße. Berichte zu wesentlichen und schädlichen Schwachstellen — selbst wenn sie nicht ausgenutzt wurden — können einen Reputationsverlust, Umsatzverluste, Vertrauensverluste und öffentliche Maßnahmen gegen globale Technologieunternehmen nach sich ziehen.

Der Vertrauensbericht 2020 ist der unentbehrliche Leitfaden für CISOs, CIOs, Führungskräfte und weitere Sicherheitsexperten, denn er vermittelt ein Bild, wie Branchen und Wirtschaftszweige Messungen durchführen, um ihre Hausaufgaben in puncto Sicherheit zu machen.

Grundlage für den Bericht bilden Daten aus der patentierten **„Attacker Resistance Score (ARS)™“ Bewertung**[1] und Informationen, die direkt aus der Crowdsourcing-basierten Sicherheitsplattform von Synack stammen und in Tausenden Sicherheitstest erfasst wurden, die bis Juli 2020 durchgeführt wurden.

Die ARS-Bewertungsskala reicht von 0 bis 100. Je höher der Wert ist, umso höher die Wahrscheinlichkeit, dass ein Unternehmen sich selbst gegen einen Cyberangriff verteidigen kann. Je geringer der Wert, umso mehr Risiken ist das Unternehmen ausgesetzt.

2020 betrug die branchenübergreifende Durchschnittsbewertung 53. Das war eine leichte Verschlechterung zum Durchschnittswert des Vorjahres von 54. Im Vertrauensbericht 2020 wird jedoch erläutert, warum sich die Bewertungen von Jahr zu Jahr ändern können. Unternehmen können eine ARS von 100 erzielen. Ein Wert über 70 ist ein starker Indikator für herausragende Sicherheitspraktiken. Die Kunden von Synack setzen eine Prämie für Sicherheitstests aus und analysieren proaktiv neue Assets und digitale Anwendungen.

Das bedeutet, dass solche Organisationen, selbst wenn die ARS zeitweise abfällt, neue Probleme in kürzester Zeit angehen können und daher im Vergleich zu Mitbewerbern in einer besseren Position sind, sich selbst zu verteidigen. Das Ziel ist nicht, die höchste Bewertung zu erzielen und dann einfach weiterzumachen, sondern fortlaufend zu messen, wie gut neue Technologien und Assets gegen Angriffe gewappnet sind. Einige Unternehmen liegen mit ihrer Bewertung über oder unter dem Branchendurchschnitt, allerdings sind die Bewertungen selbst bei den proaktivsten Unternehmen nicht gleichbleibend.

1 Die geschützte „Attacker Resistance Score“ Bewertung (ARS) von Synack ist eine Bewertung, wie gehärtet Ihre Assets gegen einen Angriff sind. Die ARS insgesamt bietet einen umfassenden Überblick über die Anfälligkeit der Ziel-Assets für einen Angriff, basierend auf einem patentierten Algorithmus, der von Synacks Data Science Team entwickelt wurde. Es handelt sich um eine Funktion aus Angriffskosten, Schwere der Feststellungen und der Effizienz bei der Behebung. Weitere Informationen zur Bewertung ARS stehen im Anhang zur Verfügung.

ATTACKER RESISTANCE SCORE™ BEWERTUNG

Eine realistische Bewertung basierend auf einem soliden Modell

„Attacker Resistance Score“ Bewertung

=

Angriffskosten

Der Arbeitsaufwand des Synack Red Team, um durch die Angriffsfläche durchzudringen und Schwachstellen zu finden

+

Schwere der Feststellungen

Der Schweregrad und die Menge an Schwachstellen, die in einem Asset gefunden wurden

+

Effizienz bei der Behebung

Wie effizient löst ein Unternehmen ermittelte Probleme in seiner Umgebung

TEIL 2

DIE WICHTIGSTEN FESTSTELLUNGEN BEIM VERTRAUEN 2020

Synack

ABBILDUNG 1: ATTACKER RESISTANCE SCORE 2020 NACH BRANCHE

Branche[2]	2018 (Vertrauensbericht Ausgabe 1)	2019	2020[3]	Vorfälle/Verstöße (Data Breach Investigation Report von Verizon)[4]
Staat	57	47	61	6843/346[5]
Finanzdienstleistungen	61	57	59	1509/448
Gesundheitswesen	56	60	56	798/521
Technologie	53	46	55	5471/360[6]
Bundesstaatliche, kommunale und Bildungseinrichtungen	49	46	50	819/228[7]
Beratung/Unternehmens- und IT-Dienstleistungen	50	53	48	7463/326[8]
E-Commerce	45	48	47	5471/360[9]
Einzelhandel	54	45	46	287/146
Verarbeitendes Gewerbe/kritische Infrastruktur	65	70	45	1070/407[10]
Durchschnitt	**56**	**54**	**53**	

Behörden verstärken Cyberabwehr

Für viele Branchen war es aufgrund der unvorstellbaren Veränderungen, die zur Eindämmung der COVID-19-Pandemie erforderlich waren, ein schwieriges Jahr. Das trifft insbesondere auf Behörden und Regierungsstellen in aller Welt zu. Diese globale Branche zeigte jedoch auch, dass fortlaufende Tests und eine schnelle Behebung entscheidend für eine effektive und herausragende Cybersicherheit sind.

Regierungsstellen erzielten im Vertrauensbericht 2020 im Branchenvergleich mit einem Wert von 61 die beste Durchschnittsbewertung. In den USA fordert die neue Richtlinie Binding Operational Directive 19-02 der Behörde für Cybersicherheit und Infrastruktursicherheit (CISA) von Regierungsstellen, kritische Schwachstellen innerhalb von 30 Tagen zu beheben. Damit reagierten Behörden schneller, um Mängel zu beheben. Und das hat einen erheblichen Unterschied gemacht. Insgesamt konnten Behörden die Zeit zur Behebung von Mängeln um 73 % verringern und beeinflussten damit die Gesamtbewertung für die Branche positiv.

2020 arbeitete Synack während der COVID-19-Pandemie mit vielen Behörden zusammen. Das Synack Red Team, unsere Community aus den weltweit besten ethischen Hackern, wurde beauftragt, sicherzustellen, dass die staatlichen Stellen gut geschützt sind, wenn neue Technologien in kürzester Zeit entwickelt werden, um den zunehmenden und dringenden Anforderungen gerecht zu werden. Viele ihrer Assets waren ein kritischer Faktor bei der Reaktion auf die Pandemie. Sie waren nötig, damit unser Land weiterhin die wichtigsten Funktionen aufrechterhalten konnte.

2 Ausführlichere Beschreibungen der einzelnen Branchen finden Sie im Anhang.

3 Januar 2019 bis Juli 2020 (Wir haben unsere Analyse aufgrund von COVID-19 verlängert.)

4 Data Breach Investigation Report 2020 von Verizon

5 Data Breach Investigation Report 2020 von Verizon: Öffentlicher Sektor

6 Data Breach Investigation Report 2020 von Verizon: Informationswesen

7 Data Breach Investigation Report 2020 von Verizon: Bildungsdienstleistungen

8 Data Breach Investigation Report 2020 von Verizon: Professionelle, wissenschaftliche und technische Dienstleistungen

9 Data Breach Investigation Report 2020 von Verizon: Kategorie der verwendeten Informationen

10 Data Breach Investigation Report 2020 von Verizon: Verarbeitendes Gewerbe, Versorgungsbetriebe

> *Die wichtigste Komponente unserer Reaktion war unser Crowdsourcing-basierter Penetrationstest. Mehr als 14.000 Teststunden — entsprechen 350 kompletten Tagen pro Jahr."*

JANET VOGEL
CISO
MINISTERIUM FÜR GESUNDHEITSPFELGE UND SOZIALE DIENSTE DER USA

Verarbeitendes Gewerbe und kritische Infrastruktur sind gefährdet

Andere Branchen hatten in diesem Jahr mit mehr Schwierigkeiten zu kämpfen. Die ARS für das verarbeitende Gewerbe und die kritische Infrastruktur verschlechterte sich 2020 auf 45, 2019 lag der Wert bei 70. Die Verschlechterung um 36 % ist im Branchenvergleich der größte Rückgang im Vertrauensbericht 2020. Einige Unternehmen in dieser Branche erreichten eine Bewertung von 90. Viele der am besten bewerteten Unternehmen setzen auf einen fortlaufenden Testansatz. Das verarbeitende Gewerbe und die kritische Infrastruktur stand unter enormen Druck, und zwar aufgrund der Veränderungen, die schnell erforderlich waren, um die Richtlinien zur Verlangsamung der COVID-19-Ausbreitung umzusetzen, und diese Belastung schlägt sich in der geschwächten Sicherheitslage nieder, denn die Branche hat weiterhin mit einer Vielzahl von Angriffen zu kämpfen.
Dem Data Breach and Investigations Report 2020 von Verizon zufolge gab es 469 große Vorfälle, die das verarbeitende Gewerbe betrafen, vorwiegend infolge von Angriffen mit wirtschaftlicher Motivation und auf den Staat als Institution. Leider sind kritische Branchen oft nicht gut geschützt, denn sie vertrauen häufig auf veraltete Systeme. In einer kürzlich von Greenbone Networks durchgeführten Umfrage unter Unternehmen in der kritischen Infrastruktur gaben nur 36 % der Befragten an, eine hohe Widerstandsfähigkeit gegen Cyberangriffe zu haben.

Die Angriffsfläche im Gesundheitssektor wurde durch COVID-19 vergrößert

Innovationen im Gesundheitswesen waren und sind elementar im Kampf gegen die Pandemie. Die Dringlichkeit, mit der neue Apps entwickelt und bereitgestellt wurden, ging ebenfalls einher mit Herausforderungen für die Cybersicherheit. Darüber hinaus berichteten Strafverfolgungsbehörden aus aller Welt einen Anstieg der versuchten Cyberangriffe auf Krankenhäuser. Trotz dieser Probleme erzielte die Branche die dritthöchste Durchschnittsbewertung, denn Forschungs- und Fertigungseinrichtungen blieben wachsam und setzten die ständigen Tests ihrer digitalen Assets fort. Einige Unternehmen konnten ihre Bewertung steigern, und zwar weil sie Tests und Behebungsmaßnahmen während der Pandemie ganz oben auf die Tagesordnung gesetzt haben. Die Durchschnittsbewertung für den Gesundheitssektor lag im Jahr 2020 bei 56, eine Verschlechterung um vier Punkte – 2019 lag der Wert bei 60. Das SRT testete zahlreiche Technologien, die direkt in Zusammenhang mit diesen Bemühungen standen. Insgesamt sind die tatsächlichen Verstöße in Krankenhäusern zurückgegangen. Das ist ein wesentlicher Gradmesser dafür, dass Sicherheitstests eine Wirkung haben.

Der E-Commerce entwickelt sich positiv infolge der stark ansteigenden digitalen Nachfrage

Der Einzelhandel und E-Commerce mussten gravierende Veränderungen in ihrem etablierten Geschäftsmodell erdulden. Der starke Nachfrageanstieg im Bereich Online-Shopping und Heimlieferservice sorgte dafür, dass die durchschnittliche ARS für den E-Commerce sich um zwei Punkte (seit 2018) verbesserte, während COVID-19 um 7 %, denn Unternehmen priorisierten Tests für neue Apps und bemühten sich um eine schnelle Behebung von Schwachstellen. Derweilen verringerte sich die ARS für den Einzelhandel um 15 %. Dieser Rückgang ist gekennzeichnet durch den wirklich herausfordernden Übergang zu einem digital-geprägten Handel während der letzten sechs Monate.

Finanzdienstleistungen kämpfen weiterhin mit massiven Unterbrechungen durch COVID-19

Trotz der massiven Bemühungen, die Arbeit von Büroeinrichtungen in Zoom-Chats zu verlagern, realisierte der Finandienstleistungssektor die zweithöchste ARS in diesem Jahr von 59 und lag damit knapp hinter dem Staat.

Die Finanzdienstleister haben sich während der Pandemie schnell verändert, um ihre Mitarbeiter dabei zu unterstützen, sich in der neuen Arbeitsrealität außerhalb des Büros zurecht zu finden, und sicherzustellen, dass Kunden weiterhin die benötigten Dienste in Anspruch nehmen konnten, während Banken und Maklerfirmen vorübergehend geschlossen waren. Fortlaufende Sicherheitstests waren ein ausschlaggebender Faktor bei der höheren ARS der Branche. Kunden von Synack, die sich einem fortlaufenden Testansatz verschrieben haben, haben eine um 18 % bessere Bewertung erzielt als andere Unternehmen.

Die digitale Transformation führt zu Rückgang bei Beratung und IT-Dienstleistungen

Die ARS ging für Beratung und IT-Dienstleistungen 2020 auf 48 zurück. Es zeigt sich in dieser Branche, dass die digitale Transformation weiterhin größere Schwierigkeiten bereitet. Die Unternehmen testen mehr Assets und entwickeln mehr Technologien. Das führt dazu, dass mehr Schwachstellen gefunden werden. Und infolge hat das Auswirkungen auf die Gesamtbewertung.

Aber der Weg hin zu Vertrauen ist nicht linear. Vielmehr zählt die Devise „Versuch und Irrtum“, und es gilt, Schwachstellen schnell zu beheben, um Veränderungen zu bewirken. Viele Unternehmen in dieser Kategorie haben den Weg durch die digitale Transformation erfolgreich beschritten und freuen sich weiterhin über verbesserte Bewertungen. Einige erzielten sogar einen Wert von 96. Die führenden Unternehmen in diesem Sektor erzielen überdurchschnittliche Bewertungen und gehen in puncto proaktives Testen anderen Unternehmen der Branche mit gutem Beispiel voran. Regierungsberater waren zum Beispiel stark damit beschäftigt, die landesweite Supply Chain abzusichern und die damit verbundenen Assets proaktiv zu testen.

TEIL 3

SICHERHEIT IN EINER UNSICHEREN UMGEBUNG

Synack

Die globale Pandemie setzte CISOs und weitere Sicherheitsexperten massiv unter Druck. Verbraucher setzten unverzüglich auf Homeoffice-Plattformen und Videokonferenz-Apps und erwarteten — oder forderten, dass Unternehmen ihre Sicherheit und Privatsphäre schützen sollten. Marken, die nicht in der Lage waren, dieses Vertrauen aufrechtzuerhalten, waren mit realen und messbaren Konsequenzen konfrontiert.

Zoom ist ein wirklich gutes Beispiel. Das Tool erlebte einen sprunghaften Anstieg bei der Nutzung in diesem Frühling, als Schulen und Unternehmen dazu übergegangen sind, von zu hause aus zu arbeiten. Seine Glaubwürdigkeit hat jedoch gelitten unter den Schlagzeilen im Wall Street Journal und der New York Times. Es wurde von massiven Schwachstellen und der Möglichkeit, dass Hacker die Plattform ausbeuten, berichtet. „Zoom Bombing“, sprich unerwünschte Eindringlinge in Videokonferenzen, wurde für Schulen und Universitäten zu einem echten Problem. Infolge erlitten die Aktien des Unternehmens quasi Schiffbruch. Unternehmen wie SpaceX, Google und das US-Militär haben daraufhin das Tool gesperrt, und Investoren machten ihrem Unmut über die Probleme beim Datenschutz und der Sicherheit Luft. Der Begriff „Zoom-Backlash“ (sprich, vielfach geäußerte Vorwürfe gegen Zoom) war plötzlich in aller Munde.

Das Management von Zoom reagierte mit einer entschlossenen PR-Kampagne und beauftragte renommierte Sicherheitsexperten als Berater in Sicherheitsfragen. Der CEO unternahm eine groß angelegte Entschuldigungsreise. Das Unternehmen hat sogar eine Cybersicherheitsfirma gekauft. Zooms Marktbewertung lag im August bei über 100 Milliarden US-Dollar. Doch die unvorhergesehenen Schwachstellen und potenzielle weitere Sicherheitsprobleme haben zahlreichen aggressiv agierenden Mitbewerbern zu einem kritischen Zeitpunkt die Tür geöffnet, als Unternehmenskunden ihrerseits darauf angewiesen waren, das Vertrauen unter ihren Kunden zu stärken.

Es ist aber nicht so, dass Unternehmen keine Möglichkeiten haben, große Schwachstellen vorauszusehen, die unweigerlich das unbezahlbare Vertrauen am Markt beschädigen. Fortlaufende Tests sind eine Möglichkeit, solchen unschönen – und schädlichen – Überraschungen vorzubeugen.

Die ARS ändert sich während andauernden Schutzmaßnahmen

Schon bald nachdem die ersten Anordnungen zu hause zu bleiben in den USA in Kraft getreten waren, verschlechterten sich die ARS-Bewertungen für einige wichtige Branchen wie Einzelhandel oder verarbeitendes Gewerbe und kritische Infrastruktur. Und auch infolge von Quarantäneanforderungen verbrachte das Synack Red Team mehr Zeit damit, bei unseren Kunden nach Schwachstellen zu suchen. Zwischen März und April 2020 verbrachte das SRT im Vergleich zum gleichen Zeitraum im Vorjahr 70 % mehr Zeit mit der Analyse von Assets.

> *"Etwas Positives hat die COVID-19-Pandemie bewirkt: Es ist klar geworden, dass Sicherheit die Grundlage für Geschäftserfolg ist."*

GREG MCCORD
GLOBAL HEAD OF INFORMATION SECURITY
CalAmp

ABBILDUNG 2: ARS-BEWERTUNGVERÄNDERUNGEN WÄHREND COVID-19

Branche	ARS-Veränderung während COVID-19†
Beratung/Unternehmens- und IT-Dienstleistungen	-3,88 %
E-Commerce	6,72 %
Finanzdienstleistungen	-11,64 %
Staat	13,46 %
Gesundheitswesen	-0,74 %
Verarbeitendes Gewerbe/ kritische Infrastruktur	-6,59 %
Einzelhandel	-7,15 %
Bundesstaatliche, kommunale und Bildungseinrichtungen	26,16 %
Technologie	6,38 %

† Synack-eigene Daten vom, 1. März bis 1. Juli 2020

> *Vertrauen ist wirklich absolut wichtig. Das heißt, dass Produktsicherheit bei uns höchste Priorität hat, damit wir das Vertrauen unserer Kunden erhalten. Als CEO und ehemaliger CISO setze ich auf Crowdsourcing-basierte Penetrationstests, um mir ein realistisches Bild aus Sicht des Angreifers von meiner Angriffsfläche zu machen. Dafür habe ich mich für Synack entschieden. Über das SaaS-Portal von Synack kann ich ganz einfach umsetzbare Ergebnisse für mein Unternehmen einsehen. Sie machen mir das Leben leicht, denn sie übernehmen auch die Prüfung und Patch-Überprüfung. Außerdem kann ich die Compliance-Felder auswählen, die ich prüfen muss."*

MICHAEL COATES
MITBEGRÜNDER UND CEO, ALTITUDE NETWORKS
EHEMALIGER CISO, TWITTER

Es ist Zeit, erheblich mehr in Sicherheit zu investieren

Während der Pandemie lag der Fokus von CISOs darauf, sicherzustellen, dass es bei zentralen Unternehmensprozesse nicht zu Störungen durch Angriffe kam. Tatsächlich gaben 70 % der in diesem Frühjahr befragten Unternehmen an, mehr Investitionen in Cybersicherheit zu planen. Gleichzeitig orientiert sich das Management mehr in Richtung Cloud als elementaren Bestandteil der Prozesse. Die Boston Consulting Group hat herausgefunden, dass 45 % der befragten Unternehmen davon ausgehen, dass in den nächsten ein bis zwei Jahren die Verlagerung von Anwendungen in die Cloud mit hoher Priorität vorangetrieben wird.

Dabei bestehen jedoch erhebliche Sicherheitsbedenken. Einer 2020 durchgeführten Umfrage von IBM Security und dem Ponemon Institute zufolge führen 19 % der Unternehmen keine Scans während einer Cloudmigration durch. Und noch besorgniserregender ist, dass 57 % der Befragten zugab, nicht zu wissen, welche Schwachstellen die größten Gefahren für ihr Unternehmen bergen.

TEIL 4

BAUSTEINE VON SICHERHEITSTESTS

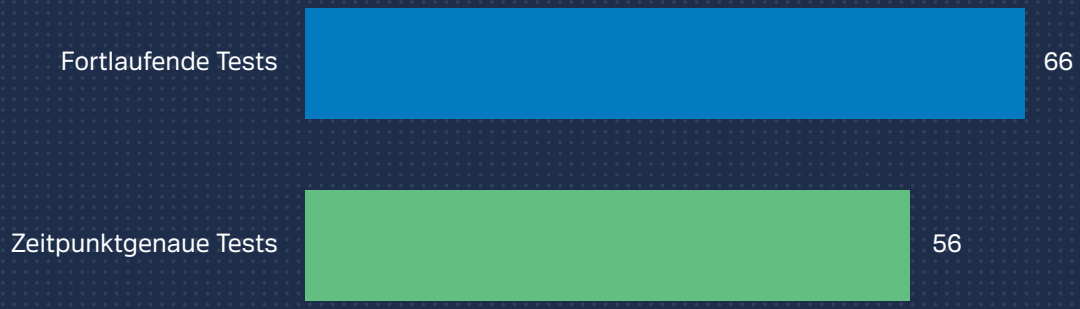
Synack

Sicherheitstests dienen einem einfachen Zweck: Potenziell schwerwiegende Schwachstellen sollen gefunden und schnell behoben werden, und die Erkenntnisse sollen dazu dienen, zukünftig besseren Code zu entwickeln.

Dieser Prozess ist allerdings komplex. Sorgfalt und Erfahrung sind die entscheidenden Schlagwörter. Um den Prozess richtig zu gestalten, benötigen Sie die weltweit besten ethischen Hacker und fortlaufende Tests, die von intelligenten, KI-gestützten Technologien durchgeführt werden. Um wirklich brauchbare Ergebnisse zu erzielen, braucht es Aufmerksamkeit und Kontinuität.

Unternehmen, die auf einen fortlaufenden Ansatz für Sicherheitstests setzen, erzielen im Schnitt eine um 18 % höhere ARS als Unternehmen, die zeitpunktgenaue Tests durchführen.

ABBILDUNG 3: ARS-BEWERTUNG FÜR FORTLAUFENDE TESTS VS. ZEITPUNKTGENAUE TESTS†



† Synack-eigene Daten

Fortlaufende Tests verbessern die ARS um bis zu 23 %

Unternehmen müssen nicht auf eine Überraschung warten. Es gibt eine bessere Möglichkeit.

Unternehmen, die einen fortlaufenden Testansatz ergreifen, erzielen im Schnitt eine um 18 % höhere ARS, manche sogar um 23 % höher, als diejenigen, die nur periodisch testen. Die Unternehmen, die ihre Assets über drei Jahre hinweg regelmäßig testeten, konnten sich freuen über einen Rückgang von:

33,3 %
WENIGER SCHWACHSTELLEN DURCH EINSCHLEUSUNG VON SQL-BEFEHLEN

30 %
WENIGER SCHWACHSTELLEN DURCH REMOTE-AUSFÜHRUNG

57 %
WENIGER SCHWACHSTELLEN DURCH CROSS-SITE-SCRIPTING

> *„Wir haben damit begonnen, Sicherheitsaspekte, die noch in unserem DevOps-Prozess angelegt waren, zu verlagern. Dabei decken wir Schwachstellen auf, die wir zuvor gar nicht gesehen haben. Außerdem finden wir neue Schwachstellen schneller. Um diese Verlagerung zu unterstützen, mussten wir ein Ökosystem rund um Sicherheitsaspekte aufbauen, damit die Entwicklungsteams schneller entsprechende Behebungsmaßnahmen anstoßen können."*

RONALD ULKO
INFORMATION SECURITY MANAGER
DOMINO'S

Arten von Sicherheitstests

SCANS
Einsatz von Software und künstlicher Intelligenz, um nach Systemen und Diensten zu suchen, die Schwachstellen aufweisen oder die nicht autorisiert wurden.

PENETRATIONSTEST
Bewertungssysteme für bekannte Schwachstellen, zum Einsatz kommt der OWASP-Standard (Open Web Application Security Project) oder andere Normungsorganisationen.

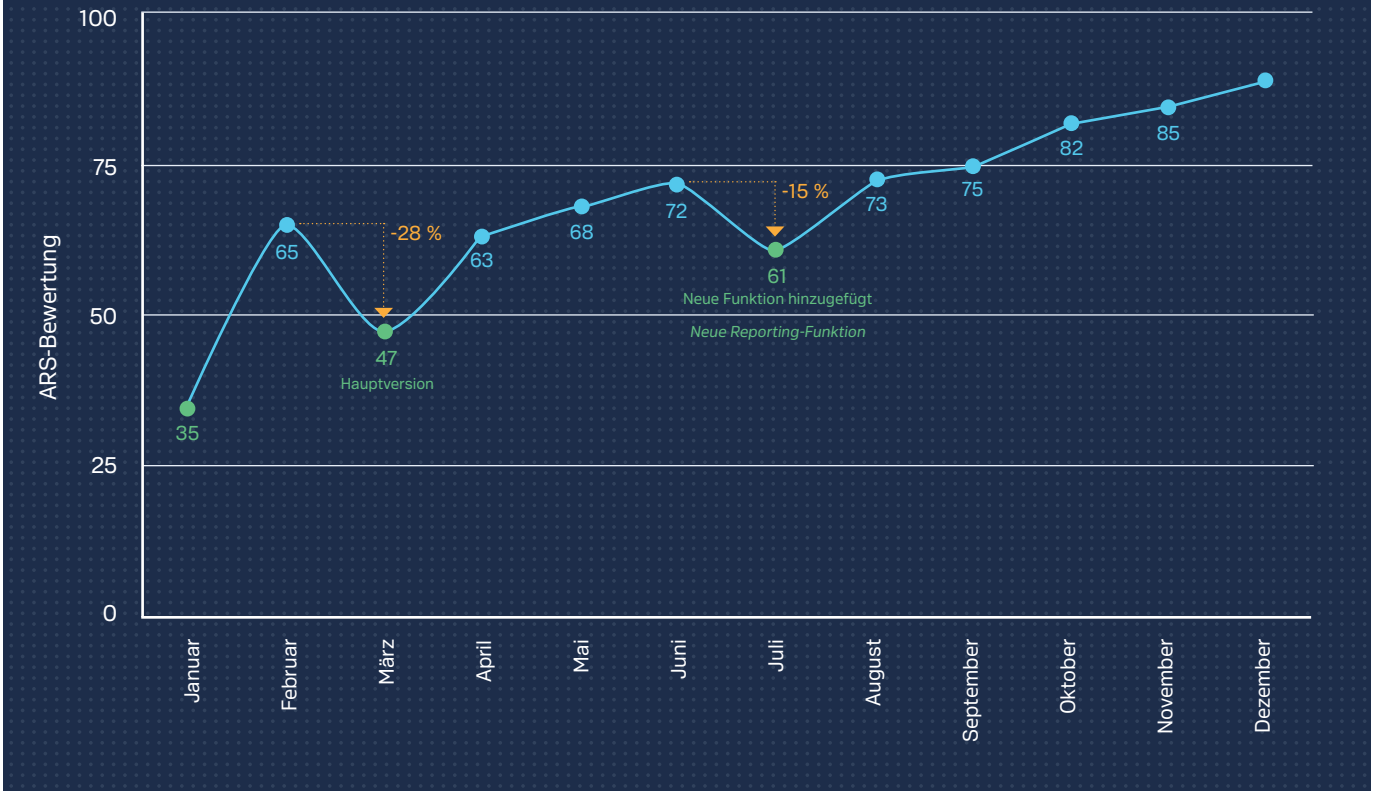
BUG BOUNTY-TESTS
Experten haben die Möglichkeit, ein Asset nach allen Regeln der Kunst anzugreifen, die Vergütung erfolgt in Form eines „Kopfgelds“ für Funde.

CROWDSOURCING-BASIERTE SICHRHEITSTEST-PLATTFORM
Ein Prozess, der die besten Elemente der drei anderen Kategorien vereint – Penetrationstests der nächsten Generation.

DER WEG HIN ZU VERTRAUEN IST NICHT LINEAR.

Die Zunahme an Agile-Teams und die häufigen Code-Releases bedingen, dass zeitpunktgenaue Tests zu kurz greifen. Für Assets, die häufig aktualisiert werden, und sensible Daten ist ein fortlaufender Testansatz erforderlich. Das ist die einzige Möglichkeit, in Echtzeit einen umfassenden Überblick über die Testumgebung eines Unternehmens zu erhalten. Dabei können Assets während der Bereitstellung bewertet werden, und Schwachstellen können entdeckt und behoben werden, bevor Angreifer sie ausbeuten können.

ABBILDUNG 4: VERÄNDERUNG DER ARS-BEWERTUNG WÄHREND DES SOFTWARE-LEBENSZYKLUS†



† Synack-eigene Daten, basierend auf zahlreichen Anwendungsfällen

Die Angriffskosten steigern

WARUM IST DAS WICHTIG

ABBILDUNG 5: DURCHSCHNITTLICHE ZEIT, EINE SCHWACHSTELLE ZU FINDEN†

Branche	Durchschnittliche Zeit für die Suche (Std.)
Gesundheitswesen	15,5
Einzelhandel	16,0
Bundesstaatliche, kommunale und Bildungseinrichtungen	16,7
E-Commerce	18,3
Finanzdienstleistungen	19,0
Beratung/ Unternehmens- und IT-Dienstleistungen	19,8
Verarbeitendes Gewerbe/kritische Infrastruktur	21,4
Technologie	29,2
Staat	30,1
Gesamt	**21,0**

† Synack-eigene Daten

Ein Großteil der Sicherheitsunternehmen — diejenigen, die im Vertrauensbericht am besten bewertet wurden — sorgen dafür, dass Angriffe gegen sie zeitaufwendig und kostenintensiv sind. Das bedeutet, dass Angreifer sich auf leichtere Zeile konzentrieren. Digitale Betrüger möchten weder Zeit, Energie noch Geld verschwenden, um in Ziele einzudringen. Wenn Unternehmen ihre Widerstandsfähigkeit gegen Angriffe verbessern möchten, müssen Sie die Angriffskosten steigern.

Angriffskosten sind eine Komponente des ARS-Modells. Dabei messen und beziffern wir den Aufwand, den ein Hacker betreiben muss, um eine Schwachstelle zu finden. Die Durchschnittszeit, um eine Schwachstelle zu finden, ist leicht zurückgegangen, von 22,8 Stunden im Vorjahr auf 21 Stunden im diesjährigen Bericht. Unternehmen testen mehr unterschiedliche Assets, einige davon enthalten sensible Daten. Experten können effektiv arbeiten, und augmentierte Tools helfen ihnen bei einer noch effizienteren Suche nach Schwachstellen. Insgesamt werden Angriffe billiger. Und das ist ein Problem. Einer kürzlich durchgeführten Studie zufolge können Angreifer einen Cyberangriff für gerade einmal 34 US-Dollar pro Monat durchführen. Manche kriminelle Cybervorgänge kosten lediglich 3.800 US-Dollar pro Monat in der Durchführung, bringen aber Erträge von bis zu 1 Million US-Dollar pro Monat.

Der Technologiesektor wies im Vergleich zu anderen Branchen mit die längste Zeit zum Finden einer Schwachstelle auf. Viele Technologiekonzerne haben eine Agile-Entwicklung eingeführt und dabei das Thema Sicherheit ganz zentral im Prozess etabliert. Damit konnten sie ihre Assets durch regelmäßige Tests härten. Infolge verblieben nach der Entwicklung weniger Schwachstellen im Code. Weiterer Pluspunkt: Die Entdeckung der eher schwerwiegenden Schwachstellen nimmt nun mehr Zeit in Anspruch.

ABBILDUNG 6: DURCHSCHNITTLICHE CVSS VON SCHWACHSTELLEN VON 2018-2020

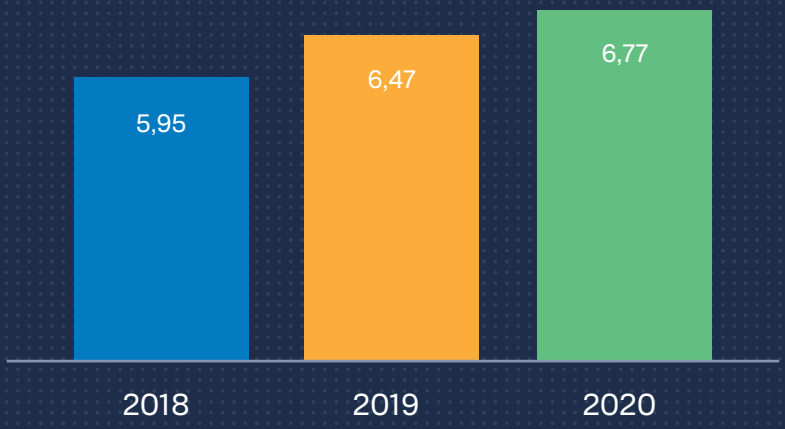


ABBILDUNG 7: DURCHSCHNITTLICHE CVSS NACH BRANCHE

Branche	Durchschnittliche CVSS
Einzelhandel	6,13
E-Commerce	6,13
Technologie	6,26
Bundesstaatliche, kommunale und Bildungseinrichtungen	6,33
Finanzdienstleistungen	6,41
Beratung/Unternehmens- und IT-Dienstleistungen	6,48
Gesundheitswesen	6,66
Staat	6,92
Verarbeitendes Gewerbe/kritische Infrastruktur	6,96

Hinweis: Abbildung 8 und 9 basieren auf Synack-eigenen Daten von 2018 bis Juli 2020.

Die Schwere der Feststellungen verstehen

Wenn Schwachstellen in einem System zur Bewertung von gängigen Schwachstellen (Common Vulnerability Scoring System, CVSS) bewertet werden, können Unternehmen und CISOs leichter verstehen, wie schwerwiegend ein Mangel ist. Diese CVSS-Bewertung ist Teil der ARS-Berechnung. CVSS-Bewertungen bieten wertvolle Informationen aber sie sind nur ein Teil der Gesamtrisikobewertung. Selbst Schwachstellen, die keine hohe Bewertung aufweisen, können zu verheerenden Sicherheitsverstößen führen. Hacker sind in der Lage, Unternehmen selbst mit primitivsten Angriffen zu kompromittieren.

Schweregrad von Schwachstellen

DIE DURCHSCHNITTLICHE CVSS IST GESTIEGEN, ABER DIE VERTEILUNG DES SCHWEREGRADS IST RELATIV UNVERÄNDERT GEBLIEBEN.

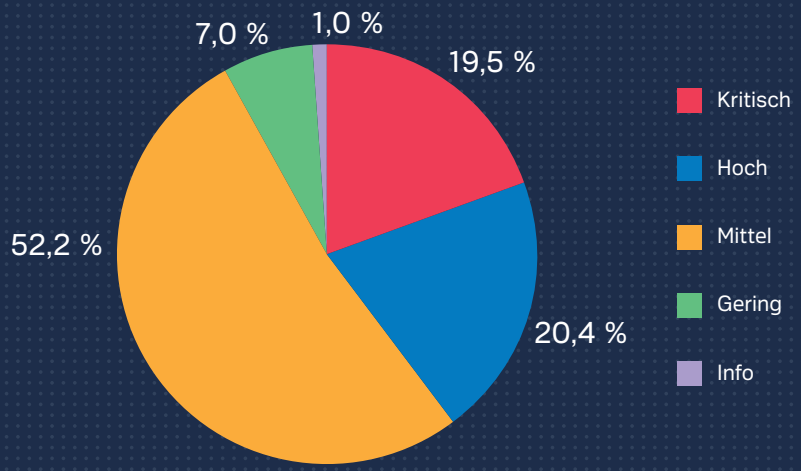
Organisationen setzen vermehrt auf das Testen verschiedener Assets, darunter auch Hostinfrastrukturen. Die durchschnittliche CVSS von Host-Assets liegt bei 7,75 und damit über der Bewertung von Internet und Mobilgeräten.

ABBILDUNG 8: DURCHSCHNITTLICHE CVSS NACH ASSET-ART

Asset-Art	Durchschnittliche CVSS
Host	7,75
Mobilgeräte	5,68
Internet	6,6

ABBILDUNG 9: VERTEILUNG VON SCHWACHSTELLEN NACH SCHWEREGRAD

Die durchschnittliche CVSS ist gestiegen, die Verteilung des Schweregrads ist jedoch relativ unverändert geblieben.



Hinweis: Abbildung 6 und 7 basieren auf Synack-eigenen Daten von 2018 bis Juli 2020.

Die Verteilung von Schwachstellen nach Kategorie

VON 2018 BIS 2020, VERTEILUNG VON SCHWACHSTELLEN, DIE SYNACK IN TAUSENDEN SICHERHEITSTEST GEFUNDEN HAT:

ABBILDUNG 10: VERTEILUNG VON SCHWACHSTELLEN NACH KATEGORIE†

Schwachstellentyp, prozentualer Anteil am Endergebnis	2018	2019
Authentifizierung/Sitzung	8 %	6 %
Authentifizierung/Berechtigung	19 %	22 %
Rohe Gewalt	2 %	2 %
Inhaltseinschleusung	5 %	3 %
Kryptografie	<1 %	<1 %
CSRF	7 %	4 %
DoS	<1 %	<1 %
Funktionale Logik	7 %	7 %
Preisgabe von Informationen	16 %	14 %
Unzureichender Transportschutz	<1 %	<1 %
Sonstige	<1 %	<1 %
Remote-Ausführung	2 %	4 %
Server-/App-Fehlkonfiguration	2 %	5 %
Einschleusung von SQL-Befehlen	5 %	8 %
Cross-Site-Scripting	26 %	23 %

† Grundlage: Synack-eigene Daten

Vertrauen verdienen, bedeutet schnell sein

ABBILDUNG 11:

Warum frühes Testen hilft

DIE KOSTEN STEIGEN SCHNELL AN, JE SPÄTER EINE SCHWACHSTELLE GEFUNDEN WIRD.

Quelle: Celerity/IBM System Science Institute+Data Breach Report – IBM Ponemon 2019

Die Unternehmen im oberen Viertel bei der ARS-Bewertung beheben Schwachstellen im Schnitt innerhalb von 30 Tagen. Schwachstellen zu beheben, ist genau so wichtig wie sie überhaupt erst zu finden. Schwachstellen früh zu finden und zu beheben, trägt zu einer erheblichen Kostenreduzierung bei.

Die Behebung ist die Dritte Komponente der ARS-Bewertung von Synack, denn dieser Aspekt ist entscheidend, um das Risiko zu senken. Da die Anzahl an Schwachstellen steigt, wird es für die Teams immer schwieriger, Schritt zu halten und alle Schwachstellen zu beseitigen. Wir empfehlen einen dreischrittigen Prozess, um Risiken effektiv zu beseitigen:

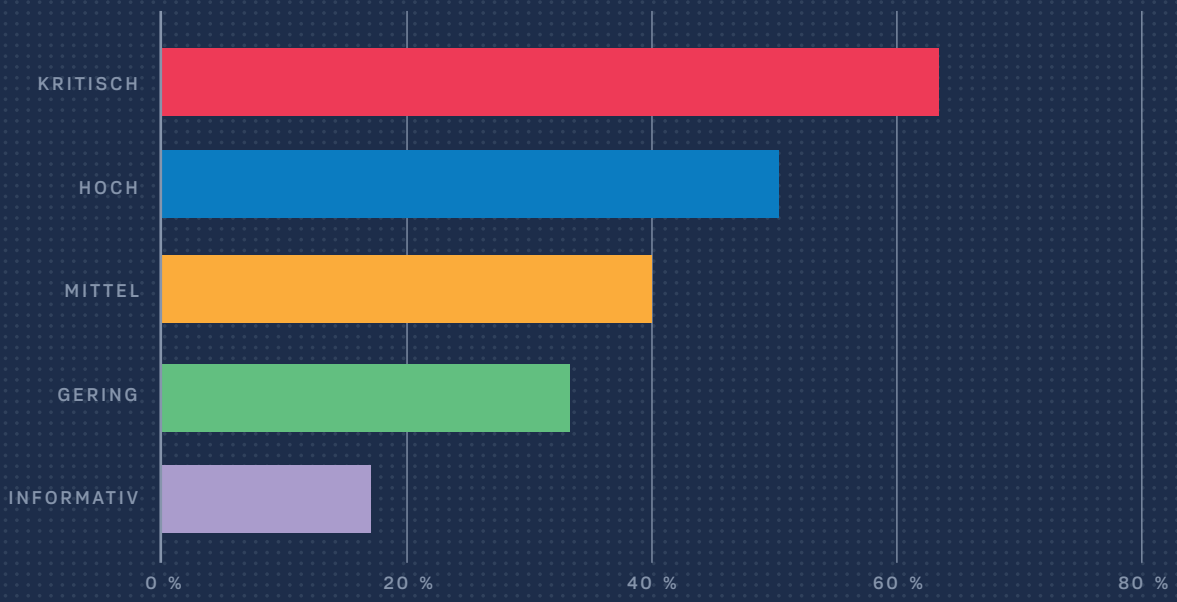
01 **Priorisieren Sie die kritischsten Schwachstellen.**

02 **Halten Sie einen umsetzbaren, wiederholbaren Behebungsprozess ein.**

03 **Implementieren Sie den Faktor Schnelligkeit in Ihren Sicherheits-Lifestyle. Das hat nachhaltige Auswirkungen.**

Kritische Schwachstellen werden als Erstes gepatcht.

ABBILDUNG 12: ANTEIL (%) AN GEFUNDENEN SCHWACHSTELLEN, DIE GEPATCHT WURDEN



Quelle: Grundlage: Synack-eigene Daten bis Juli 2020

Die Daten von Synack zeigen wenig überraschend, dass kritische Schwachstellen öfters und schneller gepatcht werden als Schwachstellen mit einer weniger kritischen Bewertung. Tausende neue Schwachstellen werden jedes Jahr entdeckt. Daher ist es wirklich eine Herausforderung, die Schwachstellen zu bestimmen, die unverzüglich gepatcht oder in ihrer Wirkung abgemildert werden müssen. Leider gaben nur 21 % der Teilnehmer der Studie von IBM Security und dem Ponemon Institute zum Patchen von Schwachstellen an, dass ihre Organisationen Mängel schnell und effektiv beheben. Der Studie zufolge kann es in manchen Fällen sogar einen Monat dauern, bis eine kritische oder hochriskante Schwachstelle in Angriff genommen wird.

Wenn Schwachstellen priorisiert werden, können Teams schneller agieren. Wenn der Fokus jedoch nur auf kritischen Mängeln liegt, bleibt die Möglichkeit unbeachtet, dass Angreifer mehrere Schwachstellen mit geringem Risiko miteinander verbinden. Das ist eine gängige und gefährliche effektive Taktik, die Angreifer nutzen, um sich Administratorberechtigungen zu verschaffen – die „Schlüssel zum Himmelreich“.

TEIL 5

FAZIT

Vertrauen ist verletzlich. Schutz ist entscheidend.

Verbraucher brauchen Vertrauen in die Marken, auf die sie täglich zurückgreifen. Und sie suchen danach auch in Institutionen. Ohne Vertrauen werden auch die besten Marken am Markt Schwierigkeiten haben, und Institutionen sind nicht in der Lage, wichtige und entscheidende Funktionen bereitzustellen, wie beispielsweise das Angebot von Gesundheitsdienstleistungen oder die Durchführung von Wahlen. Vertrauen ist praktisch das Tragwerk für alle gesellschaftlichen Aspekte – und Vertrauen vor dem Hintergrund der zunehmend schweren digitalen Bedrohungen aufrechtzuerhalten, ist eine gewaltige Aufgabe.

Es ist auch entscheidend, dass CEOs ihren Systemen vertrauen und auch den Teams, deren Aufgabe es ist, das Unternehmen abzusichern und zu schützen. In diesem Jahr hat sich gezeigt, dass Nachrichten über gefährliche Schwachstellen und massive Datenpannen zu einem immensen Reputationsschaden und zu finanziellen Verlusten führen können. Hacks und Verstöße können aber auch hohe Geldstrafen, staatliches Eingreifen und Klagen nach sich ziehen. Ein proaktiver Ansatz für Cybersicherheit ist wichtiger denn je.

Das ist die Aufgabe eines CISO. Mit der ARS steht ihnen eine Kennzahl zur Verfügung, die die Erkenntnisse bietet, die sie benötigen. Damit können sie gewährleisten, dass Unternehmen sicher sind, kostspielige Verstöße und Schwachstellen vermeiden, ihre Kunden und Partner schützen und langfristig Vertrauen und Loyalität aufbauen.

TEIL 6

VORGEHENSWEISE

Synack

Vorgehensweise – Zusammenfassung

Die geschützte Kennzahl „Attacker Resistance Score“ (ARS)™ von Synack ist eine Bewertung, wie gehärtet Assets gegen einen Angriff sind. Die ARS insgesamt bietet einen umfassenden Überblick über die Anfälligkeit der Ziel-Assets für einen Angriff, basierend auf einem patentierten Algorithmus, der von Synacks Data Science Team entwickelt wurde. Es handelt sich um eine Funktion aus Angriffskosten, den SRT-Kompetenzen, der Schwere der Feststellungen und der Effizienz bei der Behebung. Für die Berechnung der ARS werden die folgenden Dateneingaben in einer gewichteten Kombination berücksichtigt:

ANGRIFFSKOSTEN

Diese Variable dient der Beantwortung folgender Frage: „Wie viel Mühe war mit dem Versuch, in Ihre Angriffsfläche einzudringen, und der Suche nach Schwachstellen in Ihren Assets, verbunden?“ Die Angriffskosten werden für die Eingabe mithilfe aller erfassten Daten berechnet, die von LaunchPoint® erfasst werden, unsere sichere Gateway-Technologie. In den Ausgangsdaten des Testdatenverkehrs sind die gesamten Testaktivitäten des Synack Red Team für eine bestimmte Bewertung enthalten.

Bei der Berechnung der Angriffskosten isolieren wir als Erstes die bewertungsspezifischen Verkehrsdaten des Penetrationstests, um uns ein Bild von der zugrunde liegenden Struktur machen können. Anschließend berechnen wir mit diesen strukturellen Informationen die Menge an „Leistung“ oder die Mehrarbeit, die vom Sicherheitsexperten aufgewendet wurde, um erfolgreich die Schwachstelle zu finden oder um die Einschätzung zu untersuchen, dass keine Entdeckung stattgefunden hat. Die Menge der „Arbeit“ des Angreifers wird geschätzt. Dafür wird die Anzahl an „Treffern“ gezählt (d. h. HTTPS-Anfragen für Web-Apps oder Netzwerkpakete, die an Hostnetzwerke gesendet wurden) unter Berücksichtigung des Bewertungsstandorts. Gemessen wird die Zeit von der ersten Anmeldung des Sicherheitsexperten an LaunchPoint und dem Eintreffen am Bewertungsstandort bis zu dem Zeitpunkt, an dem die potenzielle entdeckte Schwachstelle gemeldet wurde bzw. wenn eine angemessene Zeit vergangen ist. Auf diese Weise werden individuelle Angriffskosten berechnet, unabhängig davon, ob die aufgewendete Mühe zu einer Schwachstelle führt oder nicht. Als Nächstes werden die Werte in einen Bereich von 1-100 normiert, und zwar unter Verwendung von organisationsübergreifenden Werten für Angriffskosten. Zuletzt bestimmt Synack die Angriffskosten für jedes Asset. Dabei wird ein Durchschnittswert der Angriffskosten für all diese Bemühungen für ein bestimmtes Asset bestimmt, unabhängig davon, ob Schwachstellen entdeckt wurden. Wurden keine Schwachstellen ermittelt, ist das ein Anzeichen für die Widerstandsfähigkeit der Bewertung gegen Cybersicherheitsrisiken.

SCHWERE DER FESTSTELLUNGEN

Abgeleitet von der Schwere und Menge der entdeckten Schwachstellen unter Berücksichtigung der Ziel-Assets. Ähnlich wie bei den Angriffskosten wird die Eingabe für die Schwere der Feststellungen für jede Schwachstelle berechnet. Dabei wird die Schwere jeder entdeckten Schwachstelle anhand einer CVSS-Skala von 0–10 gemessen. Dabei steht 0 für am wenigsten schwerwiegende Schwachstellen und 10 für wirklich schwerwiegende Schwachstellen. Basierend auf der Anzahl und der Schwere der entdeckten Schwachstellen wird eine Gruppe an linearen Modellen genutzt, um die Eingabe für die Schwere der Feststellungen für jede Schwachstelle individuell zu erstellen. Das wird anschließend weiter zusammengefasst, um eine Eingabe für jedes Asset zu erhalten.

EFFIZIENZ BEI DER BEHEBUNG

Dabei wird gemessen, wie effizient ein Unternehmen ermittelte Probleme in seiner Umgebung löst. Nach der Entdeckung von Schwachstellen werden aufseiten des Kundenziels die Daten zur Schwachstelle mit dem Kunden geteilt, damit er damit umgehen und eine Behebung erfolgen kann. Nach dem erfolgten Patchen messen wir, wie effizient der Patch ist und die Anwendungszeit, die für eine Schätzung der Behebungseffizienz vonnöten ist. Darüber hinaus berücksichtigen wir die Vielzahl und Schwere der Schwachstellen, für die Patches angewendet wurden oder die für eine folgende Weiterentwicklung der Effizienz bei der Behebung nicht berücksichtigt wurden.

Branchendefinitionen

BERATUNG/UNTERNEHMENS- UND IT-DIENSTLEISTUNGEN
Unternehmen, die sich primär auf die Veräußerung von Know-how und professionellen Dienstleistungen für Unternehmensorganisationen und Behörden konzentrieren, und nicht auf den Verkauf von Produkten.

E-COMMERCE
Unternehmen, die einen Großteil ihrer Produkte auf elektronischem Wege über das Internet verkaufen.

ENERGIE/VERSORGUNGSBETRIEBE
Unternehmen, die Energie gewinnen und bereitstellen. Diese Branche umfasst Unternehmen, die in der Erkundung und Entwicklung von Öl- oder Gasreserven, Öl- oder Gasbohrungen und -verarbeitung tätig sind, oder integrierte Energieversorger einschließlich Gas, Strom und Wasser.

UNTERHALTUNG/FREIZEIT
Unternehmen, die sich auf Erholung, Unterhaltung, Sport und tourismusbezogene Produkte und Dienstleistungen konzentrieren, darunter Talentagenturen und Musikverlage.

FINANZDIENSTLEISTUNGEN
Unternehmen, die Gelder von Einzelpersonen und anderen Unternehmen verwalten, insbesondere Kreditgenossenschaften, Banken, Kreditkartenunternehmen, Versicherungsunternehmen, Anbieter von Verbraucherkrediten.

BUNDESSTAATLICHE EINRICHTUNGEN
Bundesstaatliche Behörden, die öffentliche Programme verwalten und überwachen, wie zum Beispiel Teile des Militärs oder andere ausführende Abteilungen.

GESUNDHEITSWESEN
Unternehmen, die medizinische Leistungen sowohl für Patienten als auch für Ärzte anbieten, medizinische Ausrüstungsgegenstände oder Medikamente produzieren oder Krankenversicherungsleistungen anbieten.

VERARBEITENDES GEWERBE UND KRITISCHE INFRATRUKTUR
Fertigung von Waren für die Verwendung oder den Verkauf unter Einsatz von Arbeitskraft und Maschinen, Geräten, chemischer oder biologischer Verarbeitung oder Erstellung. Die Produkte werden vorwiegend an weitere Hersteller oder Händler verkauft. Diese Branche umfasst auch Energie- und Versorgungsunternehmen.

EINZELHANDEL
Unternehmen, die Konsumgüter oder Dienstleistungen über verschiedenste Kanäle oder Vertriebswege an Endverbraucher verkaufen, der Hauptfokus liegt auf lokal ansässigen Geschäften.

BUNDESSTAATLICHE, KOMMUNALE UND BILDUNGSEINRICHTUNGEN
Dieser Markt steht für die fünf unterschiedlichen Staatsebenen: Bundesstaat, Stadt, Landreis, Bildung und Sonderbezirke.

TECHNOLOGIE
Unternehmen, die vorwiegend Technologie oder technische Dienstleistungen verkaufen.