usd HeroLab

SECURITY ANALYSIS REPORT

2021

Wir schützen Unternehmen vor Hackern und Kriminellen.

more security. usd

INHALT

Vorwort 3

Workstation Pentests 4

Cloud Pentests 7

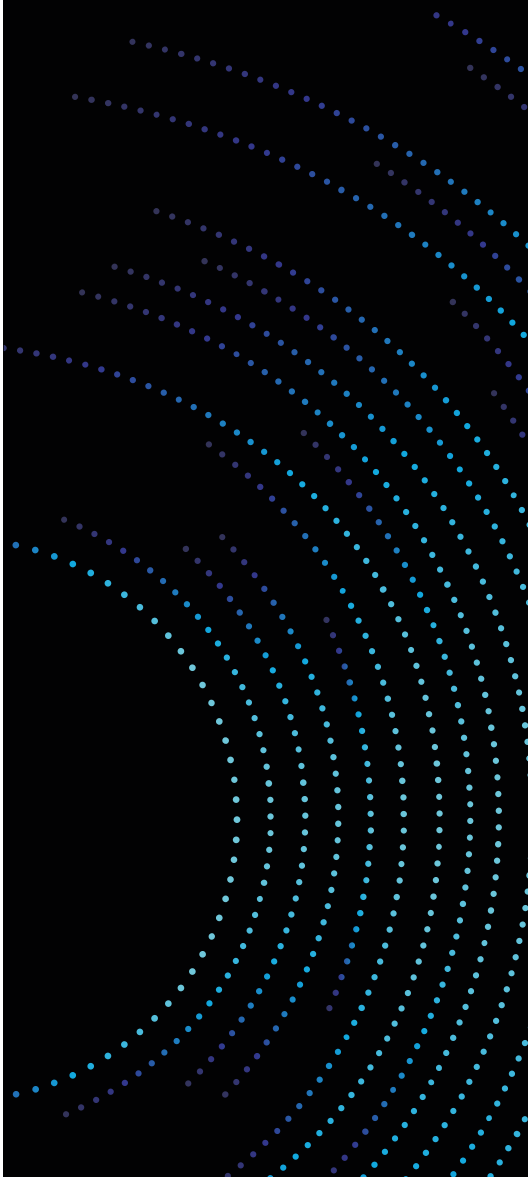
Mobile Application Pentests 10

Responsible Disclosure 14

Incident Response & Forensik 18

Next Level Reporting 21

Prognose 2022 23



SECURITY ANALYSIS REPORT 2021

2021 war hinsichtlich IT-Sicherheit ein turbulentes Jahr: Eine Vielzahl von kritischen Zero-Day-Schwachstellen, coronabedingte Auswirkungen auf das Arbeitsleben sowie die fortlaufende digitale Transformation von Unternehmen und ihren Prozessen haben viele unserer Kunden beschäftigt. Als zuverlässiger Partner für technische Sicherheitsanalysen haben wir sie dabei unterstützt.

Von **ProxyLogon** über **Printer Nightmare** bis **log4shell** kurz vor Weihnachten – in 2021 wurden zahlreiche Schwachstellen veröffentlicht, gegen die es zu diesem Zeitpunkt noch keinen wirksamen Schutz gab. Das stellte nahezu alle Unternehmen vor die Herausforderung, schnell reagieren zu müssen. Zum einen präventiv, durch Analyse und Patching, zum anderen reaktiv, um den Schaden zu bemessen und zu begrenzen. In beiden Szenarien haben wir unseren Kunden oftmals kurzfristig Hilfe geleistet – und sie anschließend längerfristig im Rahmen unserer Vulnerability Management Services begleitet.

„2021 war ein turbulentes Jahr und hat wieder einmal gezeigt, dass Cyber Security ein Prozess und kein Zustand ist. 2022 wird die Notwendigkeit, Unternehmen und Organisationen als Security Analyst*innen zur Seite zu stehen, größer als je zuvor."

Matthias Göhring
Head of usd HeroLab

Digitalisierung in Corona-Zeiten hat in Unternehmen ein zunehmendes Bewusstsein für Themen der IT-Sicherheit mit sich gebracht. Das zeigte sich beispielsweise an einer erhöhten Nachfrage nach Cloud Security-Leistungen und Sicherheitsprüfungen von mobilen Applikationen. Aufgrund der zunehmenden Arbeit aus dem Home-Office konnten wir außerdem einen deutlich wachsenden Bedarf an Workstation-Pentests beobachten, bei denen wir die Sicherheit von Arbeitsplatzgeräten prüfen.

Wir tragen eine hohe Verantwortung für unsere Kunden. Aus diesem Grund ist uns die Qualität unserer Leistungen – von Pentests über Schwachstellenscans bis hin zu forensischen Untersuchungen – enorm wichtig. Zentrale Voraussetzungen für unsere technischen Sicherheitsanalysen sind daher eine strukturierte und standardisierte Arbeitsweise, individuelle Aus- und Weiterbildung, unsere hauseigene HeroLab Toolchain und technische Topexpertise. Auf unsere Prüf- oder Audit-Berichte sind wir außerdem besonders stolz, denn wir beschreiben darin nicht nur identifizierte Schwachstellen, sondern liefern umfangreiche Informationen über alle erfolgten Prüfungen. Dadurch werden unsere Leistungen und ihre Qualität für unsere Kunden noch transparenter.

Im Security Analysis Report 2021 haben wir für Sie die Themen zusammengestellt, die unsere Kunden und uns im vergangenen Jahr besonders beschäftigt haben.

WORKSTATION PENTESTS

Auch im vergangenen Jahr ermöglichten viele Unternehmen ihren Mitarbeiter*innen die Arbeit aus dem Home-Office. Daraus ergaben sich auch für viele unserer Kunden verstärkte Sicherheitsanforderungen an Endgeräte, wie beispielsweise Laptops, die sonst nur im geschützten Unternehmensnetzwerk betrieben werden.

Insbesondere Sicherheitslücken in Anwendungen und fehlerhaft konfigurierte Systemdienste bieten ideale Einfallstore für Malware, um einzelne Computer oder ein ganzes Netzwerk zu befallen. Workstations oder Clients, wie beispielsweise Windows-Notebooks, stellen dabei häufig den Eintrittspunkt dar. Angreifende erhalten durch eine erfolgreiche Kompromittierung die Rechte der angemeldeten Nutzer*innen. In dieser Situation ist es für die Sicherheit der Domäne bzw. des gesamten Unternehmens von zentraler Bedeutung, dass sich Angreifende keine lokalen oder sogar unternehmensweiten Administratorrechte verschaffen können. Dies könnte es ihnen erlauben, sich in der Domäne weiter auszubreiten und weitere Systeme zu kompromittieren.

Neu eingeführte unternehmensweite Software oder Betriebssysteme stellen ein besonders hohes Risiko dar. Wichtige Voraussetzung ist eine sichere Konfiguration, die an renommierte Sicherheitsstandards und Best Practices angepasst wird. Nur so können unautorisierte Zugriffe verhindert werden.

Workstation Pentests

Häufige Schwachstellen

Verwundbarkeiten in Software-Komponenten

Die Anforderungen an Workstations, die von Unternehmen an Mitarbeiter*innen herausgegeben werden, sind vielseitig und komplex. Zum einen müssen Workstations es Mitarbeiter*innen erlauben, ihrer jeweiligen Tätigkeit effektiv und flexibel nachgehen zu können. Zum anderen müssen Workstations aber auch die Sicherheitsrichtlinien des Unternehmens erfüllen und vor Zugriffen innerhalb nicht vertrauenswürdiger Umgebungen geschützt werden.

Um diesen Anforderungen gerecht zu werden, verwenden Workstations in der Regel eine große Anzahl an verschiedenen Softwarekomponenten. Dabei existiert häufig eine Mischung aus interner Software, die vom Unternehmen selbst entwickelt und verwaltet wird, sowie externer Software, die bei externen Unternehmen eingekauft wird. Insbesondere in Fragen der Sicherheit, etwa bei Anti-Viren-Produkten oder VPN Clients, vertrauen viele Unternehmen auf bekannte und namhafte externe Hersteller, um ihre Anforderungen abzudecken.

Innerhalb unserer Pentests finden wir immer wieder Sicherheitslücken innerhalb von installierten Softwarekomponenten. Diese betreffen sowohl interne als auch externe Software und führen dazu, dass niedrig privilegierte Benutzer*innen ihre Berechtigungen innerhalb der Workstation ausweiten können. Das Erlangen administrativer Rechte auf einer Workstation bildet für Angreifende häufig die Grundlage für weitere Angriffe gegen die Domäne.

Unsichere Konfiguration des Betriebssystems

Die sichere Konfiguration eines Betriebssystems ist eine komplexe Aufgabe. In vielen Fällen bestehen interne Anforderungen, die Abweichungen von einer Standardkonfiguration verlangen. Dabei kann es schnell passieren, dass eine einfache Konfigurationsänderung die Sicherheit der ganzen Workstation gefährdet.

Ein häufiges Beispiel für eine unsichere Konfiguration eines Betriebssystems ist die Anbindung eines Windows-Update-Servers (WSUS) über das unverschlüsselte HTTP-Protokoll. Viele Unternehmen verwenden einen WSUS-Server, um mehr Kontrolle über das Update-Verhalten von Workstations zu erhalten. Dabei kann die Verteilung von Updates und Software genau kontrolliert und automatisiert werden. Findet diese Verteilung aber über eine ungeschützte Verbindung statt, können Angreifende Schadsoftware in Updates einschleusen.

Fehlende Härtungsmaßnahmen

Abgesehen von einer sicheren Basiskonfiguration des Betriebssystems sind auch Härtungsmaßnahmen von großer Bedeutung für die Sicherheit einer Workstation. Viele Funktionen und Protokolle werden

von Workstations aus Gründen der Rückwärtskompatibilität noch unterstützt, obwohl sie als unsicher gelten. Härtungsmaßnahmen deaktivieren oder beschränken solche Funktionen, um die Angriffsoberfläche zu reduzieren.

Die Anzahl an möglichen Härtungsmaßnahmen auf Betriebssystemebene ist groß und in der Regel können nicht alle Maßnahmen ergriffen werden, ohne die Kompatibilität mit anderer Software oder Diensten zu beeinflussen. Deswegen sind die angewendeten Härtungsmaßnahmen auf Workstations häufig mangelhaft, da die Angst vor einem Kompatibilitätsverlust die Angst vor einem Angriff überwiegt.

Um eine vollständige Übersicht über anwendbare Härtungsmaßnahmen im Kontext des eigenen Unternehmens zu erhalten, sind Audits typischerweise das Mittel der Wahl. Innerhalb von Workstation Pentests prüfen unsere Analyst*innen aber auch auf fehlende Härtungsmaßnahmen und führen in ihrem Bericht eine Übersicht hierzu auf.

„Besonders jetzt, wo sich viele Mitarbeiter*innen im Home-Office befinden und das Risiko für Phishing-Attacken zunimmt, sind Workstations zu einem beliebten Angriffsziel geworden. Von einer Workstation aus können Angreifende ihren Zugriff ausweiten und nicht nur einen einzelnen Computer, sondern bei falscher Konfiguration oder fehlenden Härtungsmaßnahmen auch das gesamte Firmennetzwerk befallen. Ich empfehle deshalb, die Sicherheit von Workstations innerhalb von regelmäßigen Pentest auf die Probe zu stellen und die Effizienz von Härtungsmaßnahmen durch ein Security Audit überprüfen zu lassen.“

Tobias Neitzel
Managing Consultant IT Security
Leistungsverantwortlicher Workstation Pentests

CLOUD PENTESTS

Für viele Unternehmen ist es heute selbstverständlich, Daten in Clouds wie AWS, Azure oder GCP zu speichern. Auch im vergangenen Jahr haben wir eine wachsende Zahl von Unternehmen dabei unterstützt, sich in der Cloud sicher aufzustellen. Denn ein Umzug in die Cloud bedeutet nicht, dass Unternehmen die gesamte Verantwortung für den Schutz ihrer Daten abgeben. Die Provider sind zwar für den Schutz der Cloud selbst verantwortlich – die Absicherung ihrer Daten bleibt jedoch Aufgabe des Unternehmens.

Die zugrundeliegende Cloud-Infrastruktur kann noch so sicher sein – werden Anwendungen in der Cloud unsicher konfiguriert, schwache Passwörter verwendet oder Berechtigungen nicht restriktiv genug gesetzt, können Angreifende diese Schwachstellen ausnutzen, um möglicherweise die gesamte Cloud-Infrastruktur zu kompromittieren.

Cloud Pentests

Häufige Schwachstellen

Unberechtigter Zugriff auf Konfigurationsdaten

Alle großen Cloud-Provider stellen für ihre virtuellen Maschinen (VMs) Metadaten-Dienste zur Verfügung. Diese sind jeweils nur aus dem lokalen Netzwerk der VM erreichbar und enthalten sensible Informationen wie Startup-Skripte, Kontozugangsschlüssel und andere Konfigurationsparameter. Durch Schwachstellen oder Fehlkonfigurationen in Anwendungen oder Reverse Proxies sind die eigentlich internen Metadaten-Dienste auch extern erreichbar. Dies geschieht zum Beispiel, wenn Anwendungen HTTP-Anfragen verschicken, die von den Eingaben der Benutzer*innen abhängen. Hierdurch ist es Angreifenden möglich, sensible Informationen auszulesen und diese für weitere Angriffe zu benutzen.

Das vermutlich größte Risiko birgt aber wohl der Diebstahl von Kontozugangsschlüsseln über den Metadaten-Dienst. Nicht selten erlauben diese eine direkte Kommunikation mit den APIs der Cloud-Provider. Je nach den verknüpften Berechtigungen, ist es ausgehend von einem kompromittierten Zugangsschlüssel möglich, Zugriff auf lateral erreichbare Dienste zu erhalten. Durch eine stetige Erweiterung der Rechte ist sogar eine Übernahme der gesamten Cloud-Umgebung denkbar.

Subdomain Takeover

Dienste, die von Cloud-Providern zur Verfügung gestellt werden und über das Internet erreichbar sein sollen, bekommen üblicherweise eine Subdomain des entsprechenden Providers zugewiesen. Da Betreiber*innen es in der Regel jedoch präferieren, ihre Produkte unter eigenen Domains verfügbar zu machen, werden für diese oft DNS-Einträge gesetzt, die auf die Subdomains der Cloud-Provider verweisen. Ändert sich nun die Subdomain in der Cloud oder wird gelöscht, beinhaltet der DNS-Eintrag des Unternehmens eine nicht mehr existierende Subdomain. Diese kann nun von Angreifenden beim Cloud-Provider neu registriert und mit eigenem Inhalt befüllt werden. Das führt dazu, dass vertrauenswürdig wirkende Subdomains zu bösartigen Inhalten führen. Denkbar wäre beispielsweise, dass Seiten mit einer Anmeldefunktion nachgeahmt werden, um Zugangsdaten zu stehlen. Häufig werden außerdem Cookies in Webanwendungen so ausgestellt, dass diese automatisch ebenfalls an Subdomains gesendet werden. Auch hierdurch lassen sich beispielhaft Accounts übernehmen. Ein weiterer Angriffsvektor ergibt sich, wenn JavaScript-Ressourcen der übernommenen Subdomain auf anderen Seiten eingebettet werden. In diesem Fall sind Angriffe wie Cross-Site Scripting durchführbar.

Risiken beim Einsatz von AWS Cognito

Der Dienst Cognito von AWS bietet eine Registrierungs- und Authentifizierungsplattform. Anwendungen können Cognito als Identity Provider einrichten und somit ihr Accountmanagement auslagern. In herkömmlichen Webanwendungen können Nutzer*innen ihre Account-Attribute, wie Name oder E-Mail-Adresse, über die jeweilige Oberfläche der Anwendung ändern. Beim Einsatz von Cognito ist es jedoch zusätzlich möglich, Änderungen an solchen Attributen direkt über die von AWS zur Verfügung gestellte Cognito User Pool API zu tätigen. Hierdurch lassen sich auch Attribute bearbeiten, die über die Anwendung selbst nicht geändert werden können, sofern diese nicht explizit über entsprechende Einstellungen in Cognito davor geschützt wurden. Zudem kann die API genutzt werden, um sich selbst neue Accounts anzulegen, wenn dies nicht explizit verboten wurde.

Solche Besonderheiten müssen Betreiber*innen von Cognito-gestützten Anwendungen bewusst sein, um sicherheitsrelevante Fehlkonfigurationen zu vermeiden. Andernfalls können sich vielseitige Schwachstellen ergeben. Werden beispielsweise Berechtigungen in der Anwendung über Cognito-Attribute verwaltet, können sich Angreifende diese selbst zuweisen, um ihre Rechte auszuweiten. Abhängig von der Implementierung der Anmeldelogik ist auch die Übernahme beliebiger Accounts ein mögliches Szenario.

„Gerade beim Einsatz neuer Dienste in Cloud-Umgebungen müssen Service-Betreibende sich der Auswirkungen der eingesetzten Technologien bewusst sein. Eine regelmäßige Überprüfung von Anwendungen und Systemkonfigurationen hilft, Sicherheitslücken proaktiv zu erkennen. Hierzu ist jedoch eine detaillierte Einarbeitung in diese Themen notwendig, die Unternehmen neben dem Tagesgeschäft oftmals kaum leisten können. Dank unserer langjährigen Erfahrung aus Pentests können wir verlässlich beurteilen, ob Sicherheitsmaßnahmen bei Ihnen effektiv umgesetzt wurden.“

Konstantin Samuel
Senior Consultant IT Security
Leistungsverantwortlicher Cloud Pentests

MOBILE APPLICATION PENTESTS

Die Bedeutung und Verbreitung von mobilen Anwendungen, konkret Apps unter iOS und Android, hat in den vergangenen Jahren stetig zugenommen. Die Bereitstellung einer App ist oft unerlässlich, jedoch können Fehler in der Entwicklung zu ausnutzbaren Schwachstellen und damit zu erheblichen Risiken führen. Sensible Informationen wie Passwörter oder besonders schützenswerte Daten werden häufig nicht sachgemäß auf dem Gerät abgelegt und sind somit nur unzureichend vor dem Zugriff durch Dritte geschützt. Dadurch ergibt sich eine hohe Gefährdung der Vertraulichkeit dieser Nutzerdaten.

Zudem kommunizieren Apps häufig über Schnittstellen mit den Systemen des Unternehmens, um Daten serverseitig abzulegen oder nachzuladen. Durch Schwachstellen in der Implementierung dieser Schnittstellen können Angreifende Nutzerdaten kompromittieren. Im schlimmsten Fall dienen diese Schnittstellen als Einstiegspunkt in das System und somit in das unternehmensinterne Netzwerk.

Mobile Application Pentests

Häufige Schwachstellen

Unsichere Kommunikation: Verschlüsselung

Mobile Anwendungen (Apps) fungieren häufig als Zugriffsmöglichkeit auf Informationen und Funktionen, welche über das Internet auf einem Server des Anbieters verfügbar sind. Eine mobile Anwendung kommuniziert hierfür in der Regel über Programmierschnittstellen, sogenannten APIs. Hierbei überträgt die Anwendung potenziell sensible Informationen wie Benutzerinformationen, Kreditkartendaten oder Firmengeheimnisse über das Internet an den Server des Anbieters.

Mobile Anwendungen werden auf Smartphones verwendet, welche uns täglich im Alltag begleiten. Es ist naheliegend und heute gängige Praxis, während der Wartezeit am Bahnhof oder im Café auf öffentliche WLAN-Netzwerke zuzugreifen. Versendet eine mobile Anwendung sensible Daten über unverschlüsselte oder unzureichend verschlüsselte Kommunikationskanäle, so können Dritte auf diese Informationen zugreifen, um diese abzugreifen oder zu verändern. Stellt man sich eine unsichere Online-Banking-App vor, so könnte dies Angreifenden ermöglichen, auf die Zugangsdaten von Nutzer*innen zuzugreifen oder etwaige Überweisungen, welche im öffentlichen WLAN durchgeführt werden, zu verändern.

Die Kommunikation von mobilen Anwendungen sollte daher nach aktuellen Industriestandards verschlüsselt sein, um die Vertraulichkeit der übertragenen Daten sicherzustellen. Dies trifft selbstredend nicht exklusiv auf mobile Anwendungen zu. Da mobile Anwendungen auf Smartphones jedoch oft in nicht-vertrauenswürdigen Kontexten wie öffentlichen WLAN-Netzwerken verwendet werden, sollte besonders bei mobilen Anwendungen und deren APIs ein Augenmerk auf der Härtung der Konfiguration der Transportverschlüsselung liegen. Insbesondere sollten keine Daten unverschlüsselt über das Netzwerk übertragen werden. Eine im Jahr 2021 in unseren Pentests häufig identifizierte Schwachstelle ist eine unsichere App Transport Security-Richtlinie bei iOS-Anwendungen, welche es je nach Konfiguration erlaubt, unverschlüsselte Verbindungen zu einzelnen Domains oder gar zu beliebigen Domains aufzubauen.

Unsichere Datenspeicherung

Im vergangenen Jahr waren die meist verbreiteten Plattformen für mobile Anwendungen Googles Android und Apples iOS. Auf beiden Plattformen haben mobile Anwendungen ein konkretes Problem, welches sie lösen müssen: Wie können sensible Daten wie Sitzungsschlüssel sicher gespeichert werden, sodass diese nicht von dritten Apps oder bei Diebstahl des Gerätes von Unbefugten ausgelesen werden können? Erschwerend kommt hinzu, dass Nutzer*innen die Erwartungshaltung haben, nicht bei jeder Verwendung der App die Zugangsdaten erneut angeben zu müssen. Daher ist im Kontext von mobilen Anwendungen eine lange Sitzungsdauer üblich. Dies wird häufig durch lange gültige Sitzungsschlüssel gelöst, welche eine mobile Anwendung verwalten

muss. Sollten Dritte Zugriff auf gültige Sitzungsschlüssel bekommen, so können sie sich unbefugt als legitime Nutzer*innen ausgeben und auf die serverseitig gespeicherten Daten zugreifen oder diese gar verändern. Bei den Sitzungsschlüsseln handelt es sich somit selbst um sensible Informationen, die einem hohem Schutzbedarf unterliegen.

Die Speicherung von sensiblen Informationen sollte stets unter Verwendung der vom jeweiligen Betriebssystem dafür vorgesehenen Möglichkeiten für die sichere Speicherung von Daten implementiert werden. Das betrifft besonders Sitzungsschlüssel, kryptografische Schlüssel und Zugangsdaten, welche in der Keychain des jeweiligen Betriebssystems abgelegt werden sollten. Sensible Daten sollten zudem ausschließlich innerhalb der vom Betriebssystem bereitgestellten Sandbox gespeichert werden und nicht in von der Anwendung erzeugten Log-Ausgaben enthalten sein.

Cross-App Kommunikation

Mobile Anwendungen können über betriebssystemspezifische Mechanismen wie Aktivitäten oder individuelle URL-Schemata untereinander kommunizieren. Implementiert eine mobile Anwendung einen solchen Mechanismus, um Eingaben in die Anwendung zu verarbeiten, so muss jede Eingabe als potenziell bösartig betrachtet und entsprechend vor der Weiterverarbeitung validiert und bereinigt werden.

Eine Möglichkeit zur Bereitstellung von Funktionalität innerhalb der App, welche von anderen Anwendungen oder von Webseiten im mobilen Browser angesprochen werden können, sind individuelle URL-Schemata. Registriert eine mobile Anwendung der usd AG beispielsweise im Betriebssystem das Schema `usd://`, so kann die Anwendung im Folgenden als Ziel von Links aus dem Web verwendet werden. Die Verarbeitung der übermittelten Daten obliegt hierbei allein der Anwendung, der Aufruf der URL `usd://jahresbericht` könnte so beispielsweise diesen Bericht in der usd AG App darstellen.

Kann die mobile Anwendung dazu gebracht werden, über ein registriertes URL-Schema Aktionen im Namen der in der App authentifizierten Nutzer*innen ohne deren Zustimmung durchzuführen, so kann dies die Integrität der Daten in der App und im Einflussgebiet der authentifizierten Nutzer*innen auf dem betroffenen Dienst erheblich gefährden.

WebView: XSS und JavaScript-Schnittstellen zu nativem Code, SSO WebView-Typ

Mobile Anwendungen können über sogenannte WebViews Webinhalte einbinden, welche entweder lokal bereitgestellt oder aus dem Internet abgerufen werden können. Eine mobile Anwendung kann hierbei Funktionalität nativ implementieren und diese dann aus dem isolierten *WebView* per JavaScript-Code verfügbar machen. Ein möglicher Anwendungsfall für eine solche Funktionalität ist das Lesen und Schreiben von Dateien auf dem Dateisystem, direkt über die App ohne Umweg über die Browser-Schnittstellen. Implementiert eine Anwendung eine solche Funktionalität und ist anfällig für das Einschleusen von bösartigem JavaScript in die im WebView eingebundene Webseite, so ist es Angreifenden potenziell möglich, mithilfe von JavaScript sensible Dateien vom Smartphone des Nutzers auszulesen.

Bei der Verwendung von WebViews innerhalb einer App sollte also möglichst auf die Bereitstellung nativer Funktionen und die Unterstützung von JavaScript verzichtet werden, sofern der darzustellende Webinhalt dies nicht erfordert. Dadurch kann die Angriffsfläche der App verringert werden. Werden entsprechende Funktionalitäten für die Darstellung eines Webinhaltes benötigt, so sollten diese nur in den notwendigen WebViews verfügbar sein und ein besonderes Augenmerk auf die sichere Implementierung gelegt werden.

Ein Sonderfall ist die Implementierung eines Single Sign-On Logins in einer mobilen Anwendung. Hierfür sollte kein eingebetteter WebView-Typ verwendet werden, welcher Zugriff auf die im WebView eingebetteten Webseiten erlaubt, da hierüber die SSO-Zugangsdaten der Nutzer*innen abgegriffen werden könnten. Stattdessen sollte auf den Standard-Browser auf dem Smartphone beziehungsweise den WebView-Typ „SFSafariViewController“ zurückgegriffen werden, welcher neben der Isolation zur eigentlichen App zudem das Fortführen der Sitzung der Nutzer*innen aus dem Browser ermöglicht.

„Bei der Entwicklung einer mobilen Anwendung sollten bewährte Industriestandards herangezogen werden. Neben den Empfehlungen der Plattformhersteller zur Implementierung einer sicheren mobilen Anwendung kann der OWASP Mobile Application Security Verification Standard (MASVS) als Referenz dienen. Der OWASP MASVS ist zudem Teil der Sicherheitsüberprüfungen bei Mobile App Scans und Mobile Application Pentests der usd AG.“

Tim Kranz
Managing Consultant IT Security
Leistungsverantwortlicher Mobile Application Pentests

RESPONSIBLE DISCLOSURE

Regelmäßig identifizieren Security Analyst*innen des usd HeroLab im Rahmen ihrer Arbeit bis dato unbekannte Schwachstellen in Produkten. Für diese sogenannten Zero-Day-Schwachstellen existieren zum Zeitpunkt ihrer Entdeckung keine Sicherheitspatches – daher hat der verantwortungsvolle Umgang mit gefundenen Schwachstellen für uns stets oberste Priorität.

Gemäß unserer Responsible Disclosure Policy informieren wir deshalb Hersteller über von uns identifizierte Schwachstellen in Standardprodukten und veröffentlichen diese in Form von „Security Advisories" verantwortungsvoll, nachdem der Softwarehersteller ein Update bereitgestellt hat. So können sich alle Unternehmen, die diese Software einsetzen, gegen die Sicherheitslücke schützen. Wir leisten damit einen wichtigen Beitrag zu *#moresecurity*, über unsere direkten Kunden hinaus.

Im Jahr 2021 haben wir insgesamt 20 Security Advisories veröffentlicht – unsere Top Drei stellen wir Ihnen vor. Um Informationen über notwendige Sicherheitsupdates international zugänglich zu machen veröffentlichen wir unsere Security Advisories auf Englisch. Mehr Details und weitere Security Advisories finden Sie hier:
https://herolab.usd.de/security-advisories

usd-2021-0032
SUSE CVE Database (suse.com)

Description

Suse's CVE database embedded third-party contents without sufficient filtering and/or encoding. Multiple incidents have been identified where Suse embedded untrusted **<script>** tags, resulting in stored Cross-Site-Scripting (XSS).

SUSE's CVE database is a website which displays information on public CVEs. The description part of CVE records is included into the website without filtering or escaping of the respective content. A malicious actor could have included JavaScript code in the description text of a CVE. This code would then have been included within a page of the SUSE CVE database and could have been misused for a stored cross-site scripting attack.

Timeline

2021-11-10: The vulnerability is identified by Christian Rellmann
2021-11-10: The vulnerability is submitted via e-mail to security@suse.com and security@suse.de at 15:09 CET
2021-11-10: Suse acknowledges vulnerability and informs us that a fix was deployed at 17:06 CET
2021-11-30: Security advisory released by usd AG

Advisory ID
usd-2021-0032

Affected Product
SUSE CVE database

Vulnerability Type
CWE-79:
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Security Risk
High

Vendor URL
https://www.suse.com/security/cve

Vendor Status
Fixed

usd-2020-0106 (CVE-2021-25273) Sophos UTM

Description

Sophos UTM is a firewall solution by Sophos. It implements a web interface that allows authenticated users to manage quarantined mails. Additionally, users can inspect the contents of mails.

The web-based interface did not filter user controlled inputs sufficiently, resulting in multiple Cross-Site Scripting (XSS) vulnerabilities.

Sophos UTM failed to sanitize the following contents of mails before reflecting them within the web interface:

- subject
- filename(s) of attached file(s)
- sender's name
- mail body (actual contents)

As the mails are persistently stored, direct result of this behavior is stored XSS.

Timeline

2020-10-07: Vulnerability reported by Daniel Hoffmann/Advisory created
2020-12-09: Sophos is not able to reproduce the reported issue
2021-02-02: We are finally able to reproduce the issue again and provide further information
2021-02-03: Sophos acknowledges that they were also able to reproduce the issue and are working on a fix
2021-05-03: Security advisory and update published by Sophos with UTM Up2Date 9.706
2021-11-30: Security advisory released by usd AG

Advisory ID
usd-2020-0106

CVE Number
CVE-2021-25273

Affected Product
Sophos UTM

Affected Version
< UTM 9.706

Vulnerability Type
CWE-79:
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Security Risk
Medium

Vendor URL
https://sophos.com

Vendor Status
Fixed

usd-2021-0001
Insecure File Handling during Group Policy Updates

Description

Windows Group Policy updates may allow low privileged user accounts to elevate their privileges by abusing symbolic file system links.

Windows Group Policies are used to control and define the working environment of users and computers within *Active Directory*. They provide a great amount of control and allow to centrally manage Windows settings that should be unified within an organization. Among others, *Windows Group Policies* allow to deploy files, folders and access permissions across domain joined computers. This functionality has found to be vulnerable against symbolic link attacks. If a new file or folder is created, or if access permissions are changed on a file within a user controlled part of the file system, a low privileged user account can redirect the operation using symbolic links. The outcome depends on the actual operation and can lead from privileged file write vulnerabilities to more dangerous privilege escalations.

The fact that *Windows Group Policy* updates follow symbolic links during file operations can be viewed as a feature, but from our point of view it is a dangerous functionality. We encountered multiple setups where symbolic links could be used to elevate permissions from low privileged user accounts to *NT AUTHORITY\SYSTEM*.

Timeline

2021-02-23: This vulnerability is reported via Microsoft Security Response Center
2021-03-08: Microsoft raise a question about our Proof-of-Concept
2021-03-14: We add additional clarification about our PoC
2021-03-24: Microsoft informs us that they finished investigating and do not consider this a security issue
2021-04-30: Security advisory released

Advisory ID
usd-2021-0001

Affected Product
Windows 10

Affected Version
Latest

Vulnerability Type
Symlink Vulnerability

Security Risk
Conditional

Vendor URL
https://www.microsoft.com

Vendor Status
Not fixed / Disputed

The behavior was reported to Microsoft in February 2021. After finishing their investigations, Microsoft informed us that they do not consider this a security vulnerability in Windows. As we identified a real-world occurrence of this behavior which led to privilege escalation, we decided to still disclose this advisory to raise awareness about this topic.

INCIDENT RESPONSE & FORENSIK

Angriffe auf digitale Infrastrukturen haben in den vergangenen Jahren stark zugenommen. Dabei setzte sich der Trend, dass Angriffe zunehmend durch professionell agierende Gruppen durchgeführt werden, im Jahr 2021 fort. In vielen Fällen haben die Angreifenden das Ziel, Ransomware – also Malware, die Systeme und Daten verschlüsselt – auszuführen und anschließend ein Lösegeld zu erpressen. Im letzten Jahr hat beispielsweise der Angriff auf die Colonial Pipeline in den USA für großen Schaden gesorgt und die Auswirkungen deutlich gemacht. Die Methoden und Werkzeuge der Angreifenden haben sich dabei in den letzten Jahren stetig weiterentwickelt.

Mehrere kritische Zero-Day-Schwachstellen, für die es zum Zeitpunkt der Veröffentlichung noch keine Sicherheitsupdates gab, haben viele Unternehmen im vergangenen Jahr auf die Probe gestellt – und uns vor die Herausforderung, schnelle Hilfe zu leisten.

Durch den Einsatz von automatisierten Scannern konnten wir einen Angriff oftmals eingrenzen und so den Aufwand für vollumfängliche, forensische Untersuchungen reduzieren. Am Ende zeigte sich: Wer sich auf den Ernstfall vorbereitet hat, kann schneller und effizienter reagieren, wenn es darauf ankommt und damit oft schlimmeres verhindern.

Reaktion im Ernstfall

Im Jahr 2021 konnten wir mehrfach Kunden in einer Situation unterstützen, die niemand gerne erleben möchte – die sich aber leider nie vollständig ausschließen lässt.

Ob es sich um eine bestätige Kompromittierung eines einzelnen Systems, eines ganzen Netzwerks oder nur um einen Anfangsverdacht handelt, in jedem Fall heißt es schnell und entschlossen zu handeln. Gleichzeitig ist eine solche Situation alles andere als alltäglich und sorgt daher für Aufregung bei allen Beteiligten. Deshalb unser erster Tipp: Bewahren Sie Ruhe. Wie Sie sich auf einen solchen Fall vorbereiten und im Ernstfall richtig reagieren können, haben wir in unserer Notfallbroschüre „Hackerangriff – Im Ernstfall schnell richtig agieren“ für Sie zusammengefasst.

„Hackerangriff – Im Ernstfall schnell richtig agieren“

Um das Ausmaß des Incidents festzustellen und über das weitere Vorgehen zu entscheiden, muss man sich zunächst einen Überblick über die betroffenen Systeme und Dienste verschaffen und versuchen zu identifizieren, welche Aktionen Angreifernde bereits vorgenommen haben. Daraus lässt sich dann ableiten, welche Informationen die Angreifenden bereits gesammelt haben, wie sie vorgehen und was ihre Absichten sein könnten. Nur wenn man diese Informationen gesammelt hat, kann man den Incident erfolgreich abschließen und Angreifende aus dem Netzwerk aussperren.

Zusätzlich zu unseren präventiven Sicherheitsanalysen wie Pentests, Red Teaming Engagements und Consulting Leistungen, unterstützen wir Sie auch, falls es zu einem Incident kommen sollte.

Wurde ich gehackt?

Am Anfang steht meistens ein Verdacht. Das können beispielsweise auffällige Log-Einträge sein, ungewöhnliche Nutzeraktivität oder externe Meldungen über dubiose E-Mails, die versendet wurden. In diesen Fällen ist noch unklar, ob tatsächlich ein Hackerangriff vorliegt und welche Systeme betroffen sind.

Wir empfehlen in diesem Fall einen Forensik-Scan. Mit Hilfe des THOR Scanners unseres Partners Nextron lassen sich schnell und unkompliziert eine Vielzahl an – potenziell – betroffenen Systemen auf Angreiferaktivitäten untersuchen. Dies ermöglicht es, mit vergleichsweise geringem Aufwand einen ersten Eindruck über das Ausmaß des Incidents zu erlangen. Der THOR Scanner analysiert vollautomatisiert alle Systeme – egal ob Windows, Linux oder macOS – auf Artefakte von Angreiferaktivitäten. Dabei werden unter anderem Registry-Einträge, Logdateien, Caches, offene Netzwerkverbindungen, DNS-Caches und vieles mehr untersucht. Als Ergebnis erstellt der THOR Scanner einen Bericht, welcher eine Einstufung und entsprechende Kategorisierung aller Findings auf dem System enthält. Anhand dieser Ergebnisse konkretisiert sich der Anfangsverdacht - oder eben nicht. Für spezifische Systeme, bei denen Hinweise auf Angreiferaktivitäten identifiziert wurden, lohnt sich dann eine vollständige forensische Untersuchung.

Forensische Analyse

Sollte sich der Verdacht konkretisieren oder Sie bereits eindeutige Anzeichen für eine Kompromittierung feststellen, führt kein Weg an einer forensischen Analyse vorbei. Dabei werden die Systeme von unseren Forensikern toolunterstützt analysiert und dabei auf sämtliche Artefakte, welche auf Kompromittierung hinweisen, untersucht. Die Ergebnisse bringen wir nach Möglichkeit in eine zeitliche Reihenfolge, um die Aktivitäten der Angreifenden nachvollziehen zu können. Die forensische Analyse schließt den Arbeitsspeicher (RAM) mit ein; deshalb sollte man ein verdächtiges bzw. kompromittiertes System niemals einfach abschalten!

ProxyLogon, Log4Shell & Co.

Wir konnten im Jahr 2021 unsere Kunden sowohl im Kontext von großen, flächendeckend ausgenutzten Schwachstellen wie ProxyLogon in Microsofts Exchange Server und der Log4Shell-Schwachstelle, wie auch in individuell zugeschnittenen Attacken mit unserer Expertise in der Incident Response unterstützen. Dazu zählen sowohl einfache Phishing-Kampagnen, welche als massenhafter Spam an Millionen E-Mail-Adressen versendet werden wie auch gezielte Angriffe auf unsere Kunden mit speziell zugeschnittenen Payloads.

Vorbereitung ist alles

Bei den von uns bearbeiteten Incidents im Jahr 2021 hat sich wieder an vielen Stellen gezeigt, dass eine gute Vorbereitung auf einen Incident und definierte Prozesse für den Umgang mit Sicherheitsvorfällen enorm wichtig sind. Durch organisatorische Vorbereitung sowie technische Maßnahmen rund um Logging, Security Policies, Security Awareness und Vulnerability Management, konnte bei unseren Kunden ein Incident oftmals sowohl früher erkannt als auch schneller, effizienter und mit mehr Einblick in die Aktivitäten der Angreifenden bearbeitet werden. Dadurch lässt sich das Ausmaß eines Incidents stark einschränken und der entstandene Schaden minimieren.

„Die Praxis zeigt: Hunderprozentige Sicherheit gibt es leider nicht. Deshalb sind wir als IT-Forensiker*innen auch dann für unsere Kunden da, wenn es trotzallem zu einem Sicherheitsvorfall kommt. Wir identifizieren Ursache, Umfang und Folgen des Angriffs und unterstützen Sie dabei, Schlimmeres zu verhindern. Wir lassen Sie nicht allein.“

Sandro Tolksdorf
Senior Consultant IT Security
Leistungsverantwortlicher Incident Response & Forensik

NEXT LEVEL REPORTING

Zu einer guten Security Analyse gehört auch ein aussagekräftiges Ergebnis. Die Mehrzahl von Pentest-Ergebnisberichten konzentriert sich auf die identifizierten Schwachstellen. Das Problem dabei: Der Umfang der getesteten Umgebung ist daraus nicht ersichtlich und für den Kunden nicht nachvollziehbar. Das reicht uns nicht.

Uns ist es wichtig, nicht nur qualitative Analysen durchzuführen, sondern unseren Kunden eine ausführliche Einschätzung der Sicherheitslage ihrer Systeme und Anwendungen zu bieten. Mit unseren Audit-Berichten machen wir unsere Analysen transparent und demonstrieren unseren Qualitätsanspruch. Im Jahr 2021 haben wir unser Reporting auf das nächste Level gehoben.

In unserem Audit-Bericht schaffen wir für Sie Transparenz

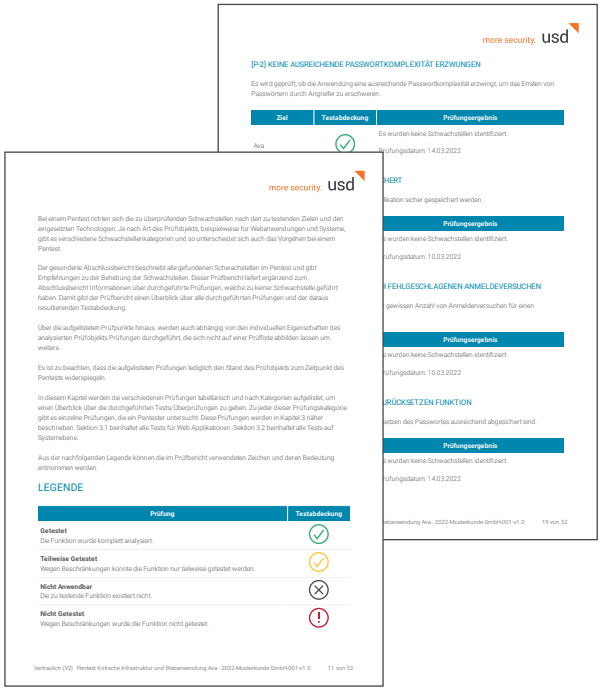
Mit steigender Nachfrage nach Pentests gibt es auch immer mehr Anbieter auf diesem Markt, wodurch es für Unternehmen schwierig ist, Unterschiede in der Qualität von Pentests zu bewerten – und das idealerweise vor Vertragsabschluss. Grund dafür ist, dass die Durchführung des eigentlichen Pentests aus Sicht des Auftraggebers weiterhin eine Blackbox ist: In einem Ergebnisbericht wird lediglich dokumentiert, welche Schwachstellen im Rahmen des Pentests identifiziert wurden. Der Bericht enthält keine Information darüber, ob und in welchem Umfang eine Funktion getestet wurde. Unserer Audit-Bericht schafft mehr Transparenz: Er ist ein zusätzliches Dokument, das den Umfang sowie das Ergebnis der Durchführung zusammenfasst. Wir zeigen dort, welche Angriffsvektoren im Zusammenhang mit welchen Funktionen getestet wurden und mit welchem Ergebnis – auch wenn dort keine Schwachstelle identifiziert wurde. Somit erhalten Sie Klarheit und können die Qualität unserer Analyse bewerten.

Nachvollziehbare Pentest-Ergebnisse

Die beste Sicherheitsanalyse bringt keinen Mehrwert, wenn die Erkenntnisse nicht nachvollziehbar und übersichtlich dargestellt sowie mit konkreten Handlungsempfehlungen versehen werden. Aus diesem Grund haben wir unsere Pentest-Ergebnisberichte grundlegend überarbeitet und um viele nützliche Informationen ergänzt. Durch Kategorien könnten grundlegende Probleme erkannt werden. Zum Beispiel: Viele Findings im Bereich „Umgang mit Benutzerdaten“ innerhalb einer Webanwendung deuten auf fehlende Awareness der Entwickler*innen für Injection-Angriffe hin. Insgesamt haben wir die Struktur und Darstellung der Ergebnisse in unserm Bericht überarbeitet und interne Referenzen ergänzt – alles für eine bessere Lesbarkeit.

Reporting angepasst an Ihre Bedürfnisse

Die Ergebnisse der technischen Analyse führen zu umfangreichen Folgemaßnahmen beim Auftraggeber: Die Ergebnisse müssen unternehmensintern weiterverarbeitet werden. Aufgabenpakete müssen den richtigen Ansprechpartner*innen zugewiesen werden. Maßnahmen zur Behebung müssen installiert, nachverfolgt und dokumentiert werden. Viele Unternehmen nutzen dafür eigene Systeme, zum Beispiel auf Basis von Jira. Dafür können wir unkompliziert eine tabellarische Zusammenfassung der Ergebnisse in einem passenden Format für den Import zur Verfügung stellen. Auf Wunsch können wir auch unternehmenseigene Vorlagen für die Dokumentation von Pentest-Ergebnissen verwenden.



Auszug aus Audit-Bericht der usd AG

PROGNOSE 2022

Das Thema Cyber Security war nie relevanter als heute. Cyberangriffe auf öffentliche und private Organisationen haben in den letzten Jahren an Häufigkeit und Qualität zugenommen – der Krieg in der Ukraine führt hier zu einer neuen Dimension. Viele Unternehmen stehen in diesem Kontext vor einer neuen, nicht greifbaren Bedrohung durch Angriffe auf ihre digitalen Systeme. Insbesondere kritische Infrastrukturen sind im Fokus. Der Bedarf an Sicherheitslösungen wie an Cyber-Security-Expert*innen ist daher so groß wie nie. Lehre, Forschung und Wirtschaft sind in der Pflicht hier gemeinsam zu agieren, um diesen Herausforderungen gerecht werden zu können – denn wir schützen Unternehmen vor Hackern und Kriminellen.

Als Unternehmen verstärken wir unser Engagement in Forschung und Lehre daher massiv, um langfristig Verantwortung für die Gesellschaft zu übernehmen. Gleichzeitig fließen viele unserer Ressourcen in die bedarfsgerechte Entwicklung unserer technischen Analysen und einen transparenten, nachvollziehbaren Audit-Bericht. Damit ermöglichen wir erstmalig mess- und quantifizierbare Qualität von technischen Sicherheitsanalysen im Cyber-Security-Markt. 2022 wird das Sicherheitsniveau vieler Organisationen auf den Prüfstand stellen. In diesem Jahr wird es daher mehr als je zuvor darum gehen, das Management von Schwachstellen dauerhaft und nachhaltig in den Prozessen von Unternehmen zu verankern.

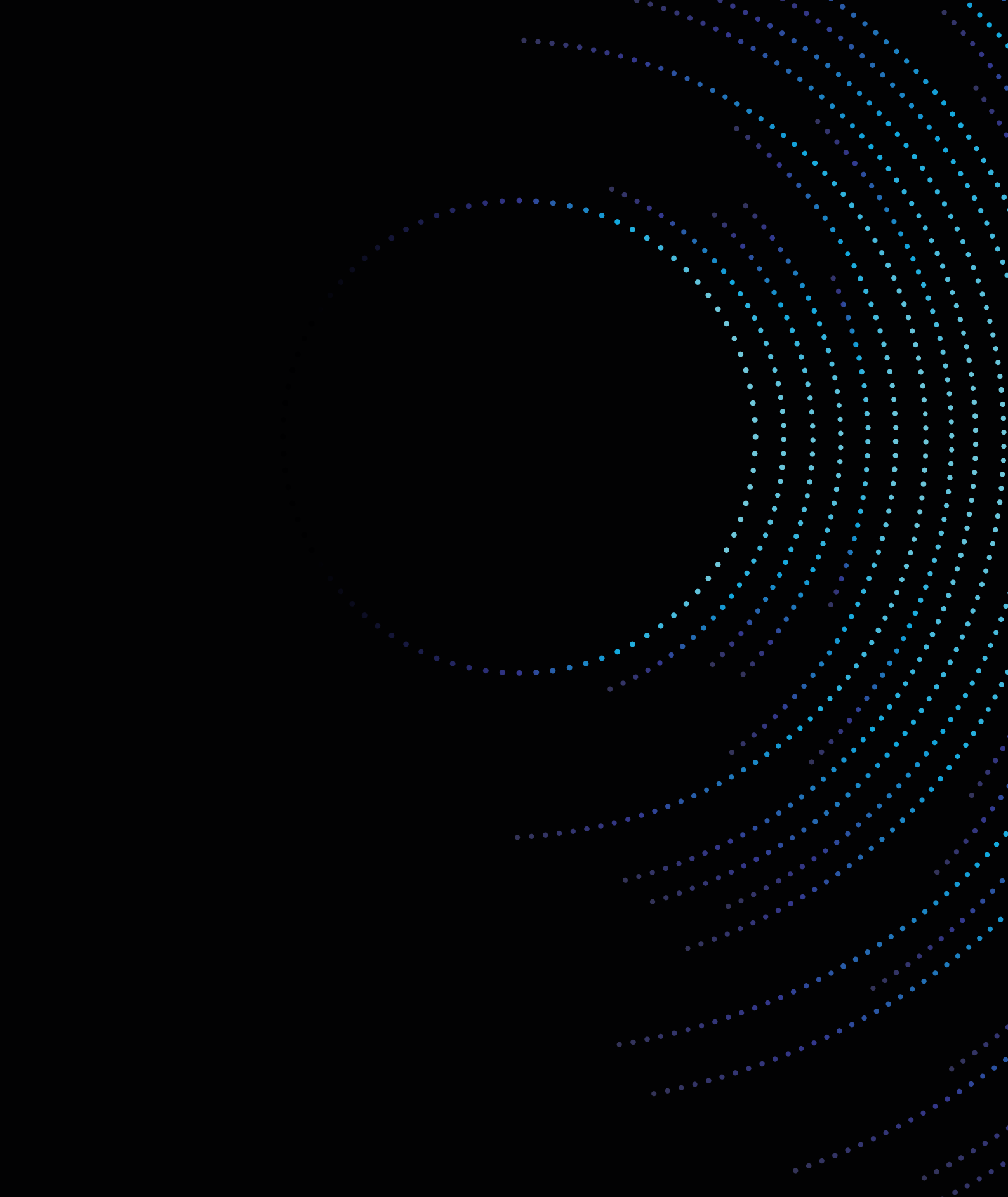
„Die Bedrohung durch Cyberangriffe ist real und größer als je zuvor. Der immensen Verantwortung, die wir als Security Analysten in diesem Kontext tragen, sind wir uns bewusst – und tun alles dafür, ihr in jeder Hinsicht gerecht zu werden. Wenn Sie uns brauchen, sind wir da.“

Stephan Neumann
Head of usd HeroLab

Unsere Expert*innen haben 2021 mehr Anwendungen und Systeme auf Sicherheitsschwachstellen geprüft als je zuvor und umfassende Ergebnisberichte zu ihren Analysen geliefert. Damit beginnt für viele Unternehmen die tatsächliche Herausforderung jedoch erst. Wie ist mit den Ergebnissen umzugehen? Wie lassen sich Fortschritte messen? IT-Infrastrukturen werden immer komplexer und Bedrohungslagen immer kritischer – da fehlen häufig schlicht die Kapazitäten, technische Sicherheitsanalysen über alle Abteilungen und Systeme hinweg fachgerecht zu begleiten und resultierende Maßnahmen nachhaltig umzusetzen. Mit unseren Vulnerability Management Services helfen wir Unternehmen dabei, Cyber Security dauerhaft in ihre Betriebsprozesse zu integrieren. Dieses Ziel mit möglichst vielen unserer Kunden zu erreichen wird 2022 eine unserer größten Aufgaben sein.

Sie benötigen weitere Informationen oder Unterstützung? Wir helfen Ihnen gerne.

Telefon: +49 6102 8631-190
Mail: vertrieb@usd.de | Kontaktformular



usd AG

Frankfurter Str. 233, Haus C1 | 63263 Neu-Isenburg
Telefon: +49 6102 8631-0 | Mail: kontakt@usd.de
www.usd.de | herolab.usd.de