IT-SICHERHEITSSTUDIE

CloudDrain

Ergebnisse einer globalen IT-Sicherheitsstudie zur Sicherheitslücke

« ownCloud / Nextcloud Unprotected Data Directory »

Sascha Brendel · Anna Brendel

LEDNERB

Inhalt

© 2024 Lednerb IT-Security GmbH

Vorwort

In unserer sich ständig wandelnden digitalen Welt muss die Sicherheit von IT-Systemen ein zentrales Anliegen für Unternehmen jeder Größe und Branche sein.

Unsere umfassende Studie beleuchtet eine kritische Sicherheitslücke in ownCloud- und Nextcloud-Instanzen und bietet tiefe Einblicke in die Risiken und Herausforderungen, denen Organisationen gegenüberstehen. Wir haben festgestellt, dass viele Unternehmen, von kleinen Firmen bis hin zu großen Institutionen, unzureichend auf den Umgang mit Cybersicherheitsbedrohungen vorbereitet sind. Unser Responsible Disclosure Prozess zeigte deutlich, dass die Kommunikation zwischen Sicherheitsforschern und Unternehmen oft durch Mängel in den Kommunikationskanälen erschwert wird.

Um diese Lücke zu schließen, empfehlen wir die Implementierung einer `security.txt`-Datei, wobei unsere Dienstleistungen eine maßgeschneiderte Lösung zur Maximierung der Sicherheit bieten. Wir hoffen, dass unsere Erkenntnisse und Empfehlungen dazu beitragen werden, die digitale Landschaft sicherer zu machen.

LEDNERB

Lednerb IT-Security - Ihr Partner für IT-Sicherheit

Es ist unser Anliegen die Infrastruktur unserer Kunden bestmöglich und effizient vor Cyber-Bedrohungen aller Art zu schützen. Wir sehen unsere Kunden als Partner und streben eine langfristige und vertrauensvolle Zusammenarbeit an.

Mit über einem Jahrzehnt Erfahrung im Bereich Web- und IT-Sicherheit haben wir uns darauf spezialisiert, den besonderen Anforderungen unserer Kunden gerecht zu werden.

Unser Ziel ist eine nachhaltige, effektive und langfristige Kooperation. Dabei bieten wir individuelle, zielgerichtete Lösungen, die sowohl für große als auch für kleine Unternehmen geeignet sind.

UNSERE DIENSTLEISTUNGEN

Managed Schwachstellenscan

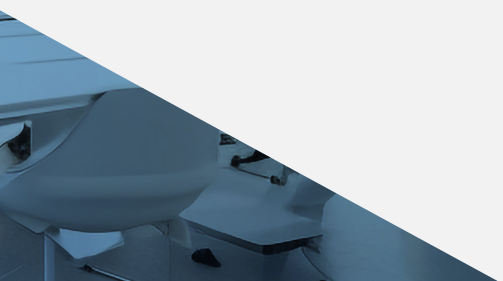
Ein Schwachstellenscan ist eine essenzielle IT-Sicherheitsmaßnahme zur Überprüfung des Sicherheitsniveaus von Systemen und Anwendungen. Bei einem Schwachstellenscan werden diese automatisiert von einem Schwachstellenscanner auf öffentlich bekannte Sicherheitslücken geprüft. Aufgrund der täglich steigenden Anzahl an Sicherheitslücken steigt ebenfalls die Anzahl an Tests, die bei einem Scan durchgeführt werden. Die Scanner-Ausgaben werden von IT-Security Analysten ausgewertet und bezüglich des jeweiligen Risikos eingeordnet.

Penetrationstest (extern / intern)

Ein Penetrationstest, kurz auch Pentest genannt, ist eine IT-Sicherheitsmaßnahme mit dem Ziel, das Sicherheitsniveau von Systemen und Applikationen zu überprüfen. Mit Hilfe eines Pentests werden sowohl offensichtliche als auch verborgene Schwachstellen erkannt und bewertet. Die Ergebnisse werden zusammen mit entsprechenden Handlungsempfehlungen in Form eines Reports zusammengefasst.

IT-Sicherheitsberatung

Wir legen Wert auf eine individuelle, zielgerichtete und umfassende Beratung und bieten Ihnen unser Fachwissen zu Themen der IT-Sicherheit und des Datenschutzes an. Wir beantworten Ihre Fragen und beraten Sie gerne u.a. zu folgenden Themen: Sicherung und Wiederherstellung von Daten, Entwicklung von Sicherheitsstrategien, Erstellung von Bedrohungsanalysen, Vorgehensweise bei Schwachstellenmeldungen, Minimierung von Abhängigkeiten zu Drittanbietern, Verschlüsselung von Dateien und E-Mails, etc.



Kurzübersicht

Cloud Computing und Cloud Collaboration stellen heute nicht mehr nur Trends, sondern fest etablierte Technologien dar, die Unternehmen jeder Größe bei der Digitalisierung unterstützen. Besonders im Bereich der Online-Zusammenarbeit bieten Cloud-Dienste eine Vielzahl von Möglichkeiten zur Effizienzsteigerung.

Self-Hosted Alternativen: ownCloud und Nextcloud

Neben den großen Playern im Cloud-Markt wie Microsoft und Google existieren Open-Source-Alternativen wie ownCloud und Nextcloud. Diese bieten Unternehmen die Möglichkeit, die Kontrolle über ihre Daten zu behalten und gleichzeitig von den Vorteilen der Cloud zu profitieren.

Sicherheitslücken in Cloud-Diensten: Ein ernstzunehmendes Risiko

Jedoch sind diese Systeme nicht frei von Risiken. Die spätestens seit 2016 bekannte Sicherheitslücke « ownCloud / Nextcloud Unprotected Data Directory » stellt hierbei ein signifikantes Risiko dar. Die Lücke tritt in der Regel aufgrund einer Fehlkonfiguration des Webservers auf und ermöglicht den unautorisierten, freien Zugriff auf sämtliche Daten aller Benutzer.

ownCloud / Nextcloud Unprotected Data Directory

Bei inkorrekter Konfiguration des Webservers ist es möglich, durch einen einfachen Webaufruf auf Log-Dateien wie
`http://cloud.example.org/data/nextcloud.log` oder
`http://cloud.example.org/data/owncloud.log` zuzugreifen.

Aus diesen Log-Dateien können dann sensible Benutzer-Informationen extrahiert werden. Dies ermöglicht im weiteren Verlauf den Zugriff auf sämtliche vom Benutzer gespeicherten Daten.

Hierfür ist ein simpler Aufruf im Webbrowser nach folgendem Muster ausreichend:
`http://cloud.example.org/data/EXAMPLE_USER`

Studienziel und Methodik

Das Ziel dieser Studie ist die Untersuchung des Ausmaßes der Sicherheitslücke « ownCloud / Nextcloud Unprotected Data Directory ».

Insgesamt wurden 921.220.480 Domains analysiert. Darunter wurden über 255 Millionen Domains aus den europäischen Ländern und über 655 Millionen Domains aus dem `.com`-Domainbereich gescannt.

Zur Datenerhebung wurde ein eigens entwickelter, hochperformanter Scanner eingesetzt, der spezifisch auf diese Sicherheitslücke ausgerichtet ist.

Der Scanner wurde als Open-Source-Projekt von uns veröffentlicht.

Responsible Disclosure Verfahren

Ein wichtiger Bestandteil dieser Studie ist die Einhaltung des Responsible Disclosure Verfahrens.

Nach der Identifizierung verwundbarer Systeme wurde versucht, die betroffenen Unternehmen und Institutionen zu kontaktieren, um sie über die Sicherheitslücke und die damit verbundenen Risiken zu informieren.

Dieser Ansatz dient nicht nur dem Schutz der betroffenen Systeme, sondern auch der Förderung eines verantwortungsbewussten Umgangs mit Sicherheitslücken.

Was ist eigentlich Responsible Disclosure?

*Responsible Disclosure ist ein zentraler Begriff in der Welt der **IT-Sicherheit**. Es handelt sich um ein Verfahren, bei dem **Sicherheitslücken** vertraulich gemeldet und behoben werden, bevor sie öffentlich bekannt werden. Dieser Ansatz basiert auf drei Säulen: **Vertraulichkeit**, **Zusammenarbeit** und einem festgelegten **Zeitrahmen**.*

*Die Hauptziele des Responsible Disclosure sind der **Schutz der Nutzer** und die **Verhinderung von Missbrauch** durch Cyberkriminelle. Eine der größten Herausforderungen besteht darin, die Interessen von Forschern, Unternehmen und der Öffentlichkeit auszugleichen sowie einen angemessenen Zeitrahmen für die Behebung der Sicherheitslücke festzulegen.*

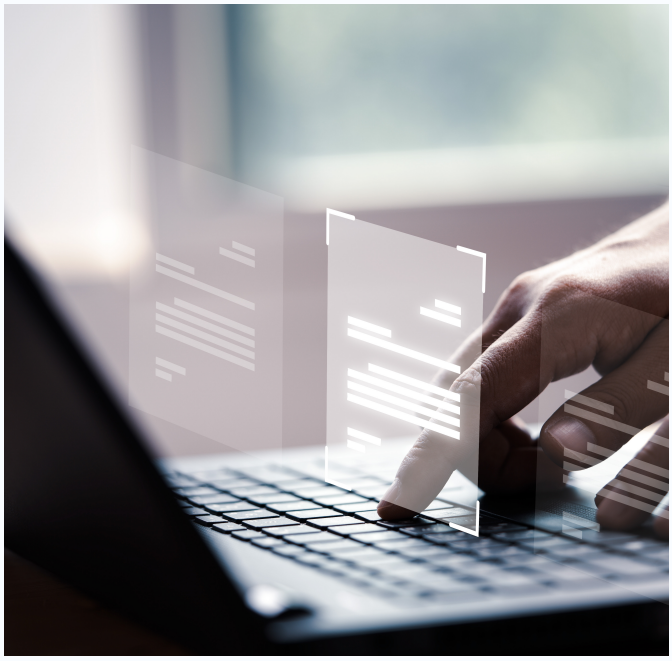
*Der typische Prozess des Responsible Disclosure umfasst die **Entdeckung der Sicherheitslücke**, die **vertrauliche Meldung** an das betroffene Unternehmen, die **gemeinsame Behebung** des Problems und schließlich die **Veröffentlichung** der Informationen nach der Problembehebung. Dieser Prozess spielt eine entscheidende Rolle in der Aufrechterhaltung der Cybersicherheit und im Schutz der digitalen Infrastruktur.*


Cloud-Dienstleistungen
& Online-Collaboration

Was ist Online-Collaboration?

Online-Collaboration bezeichnet die Möglichkeit, über das Internet gemeinsam an Projekten, Dokumenten oder anderen Aufgaben zu arbeiten. Diese Art der Zusammenarbeit ermöglicht es Teams, unabhängig von ihrem geografischen Standort, in Echtzeit zu kommunizieren und gemeinsam an Projekten zu arbeiten. Die Werkzeuge, die hierfür eingesetzt werden, umfassen häufig Funktionen wie Dokumentenfreigabe, Video- und Audio-Konferenzen, Projektmanagement und vieles mehr.

Unterstützung bei der Digitalisierung von Unternehmen



Diese Online-Collaboration-Tools spielen eine entscheidende Rolle bei der Digitalisierung von Unternehmen. Durch die Bereitstellung von Plattformen für die effiziente Kommunikation und Zusammenarbeit erleichtern sie den Übergang von traditionellen Arbeits-methoden zu modernen, digitalisierten Prozessen. Sie ermöglichen nicht nur die Automatisierung manueller Aufgaben, sondern fördern auch die Teamarbeit und steigern die Produktivität. Dies ist insbesondere in der aktuellen Ära der Remote-Arbeit von unschätzbarem Wert.

Etablierte Anbieter am Markt

Es gibt eine Vielzahl von Anbietern, die Tools für Online-Collaboration zur Verfügung stellen. Einige der bekanntesten Lösungen sind:

Microsoft Teams

Video-Konferenzen, Dateifreigabe und Integration mit anderen Microsoft-Produkten

Slack

Chat, Audio-Kommunikation und Integrationen mit anderen Diensten

Google Workspace

E-Mail, Kalender, Video-Konferenzen sowie diverse Office-Tools

Zoom

Video-Konferenzen, Funktionen für Screen-Sharing und andere Formen der Zusammenarbeit

Atlassian

Projektmanagement, Ticketsystem, Code-Verwaltung und Wissensmanagement

Datenschutz & Datensouveränität

Während Online-Collaboration-Tools zahlreiche Vorteile in Bezug auf Effizienz und Produktivität bieten, werfen sie auch wichtige Fragen in Bezug auf Datenschutz und Datensouveränität auf. Viele der großen Anbieter, wie Microsoft und Google, sind US-amerikanische Unternehmen und unterliegen damit der Gesetzgebung der Vereinigten Staaten, die in einigen Aspekten weniger strenge Datenschutzbestimmungen hat als die Europäische Union. Dies kann insbesondere problematisch sein, wenn es um die Speicherung sensibler oder personenbezogener Daten geht.

ownCloud & Nextcloud als self-hosted / managed Alternativen

ownCloud und Nextcloud sind zwei prominente Open-Source-Lösungen für File-Sync und Online-Collaboration. Im Gegensatz zu den Cloud-Diensten von US-amerikanischen Anbietern können ownCloud und Nextcloud auf eigenen Servern oder in einem Rechenzentrum des Vertrauens gehostet werden. Dies gibt Unternehmen und Organisationen eine höhere Kontrolle über ihre Daten und stärkt die Datensouveränität.

Managed Instanzen

Einige Anbieter bieten "Managed" ownCloud- oder Nextcloud-Instanzen an. In diesem Fall übernimmt der Dienstleister die Installation, Wartung und Aktualisierung der Software, während das Unternehmen sich auf seine Kernkompetenzen konzentrieren kann. Diese Dienstleistungen können sowohl im eigenen Rechenzentrum des Unternehmens als auch bei einem externen Dienstleister gehostet werden.

Self-Hosted Instanzen

Bei einer self-hosted Instanz liegt die volle Verantwortung für Installation, Wartung und Sicherheit beim Unternehmen selbst. Dies erfordert zwar mehr Fachkenntnis, bietet jedoch maximale Kontrolle über die Daten und die Infrastruktur.

Vorteile gegenüber US-Anbietern

- **Datensouveränität**: Da die Daten in einem eigenen Rechenzentrum oder bei einem vertrauenswürdigen, lokalen Anbieter gespeichert werden, wird die Abhängigkeit von ausländischen Rechtsordnungen minimiert.
- **Datenschutz**: Durch die Kontrolle über die eigenen Server können strengere Datenschutzrichtlinien und -technologien implementiert werden, die dem EU-Recht entsprechen.
- **Anpassbarkeit**: Als Open-Source-Lösungen bieten ownCloud und Nextcloud die Möglichkeit, die Software an spezifische Bedürfnisse und Anforderungen anzupassen.
- **Kosten**: Im Vergleich zu lizenzpflichtigen Lösungen können Open-Source-Alternativen auf lange Sicht kosteneffizienter sein, insbesondere wenn sie selbst verwaltet werden.

« ownCloud / Nextcloud Unprotected Data Directory »

Ablauf des Angriffs

Schritt 1

Download der Log-Datei

Die Log-Datei kann bereits sensible Informationen enthalten, u.a. Benutzer-, Verzeichnis- und Dateinamen.

Schritt 2

Extraktion von Nutzernamen

Die erbeuteten Benutzernamen lassen sich auch für weitere Angriffe sowie Phishing-Kampagnen nutzen.

Schritt 3

Aufruf des Verzeichnisses

Durch einen einfachen Aufruf einer URL im Webbrowser erhält ein Angreifer Vollzugriff auf alle gespeicherten Daten.

Aufgrund einer Fehlkonfiguration des eingesetzten Webserver kann ein Angreifer im Extremfall auf alle in der jeweiligen Cloud gespeicherten Dateien zugreifen. Hierfür muss der Angreifer keine Anmeldedaten kennen oder komplizierte Hacking-Verfahren anwenden.

Schwachstellenbeschreibung

Die Sicherheitslücke « ownCloud / Nextcloud Unprotected Data Directory » resultiert aus einer Fehlkonfiguration des Webservers. Dies ermöglicht den ungeschützten Zugriff auf sensible Log-Dateien und eventuell auch Benutzerdaten. Je nach Ausmaß der Fehlkonfiguration können die Auswirkungen variieren:

- **Zugriff auf Log-Dateien:** In diesem Fall sind sensible und personenbezogene Daten potenziell gefährdet. Aus den Log-Dateien können ggf. Benutzernamen extrahiert werden.

- **Kritische Fehlkonfiguration:** Bei einer besonders schwerwiegenden Fehlkonfiguration ist der Zugriff auf einzelne Benutzerverzeichnisse möglich. Ein unautorierter und unauthentifizierter Angreifer kann dann auf sämtliche gespeicherte Daten, verschiedene Dateiversionen und sogar "gelöschte" Dateien, die sich noch im Papierkorb befinden, zugreifen.

Ursachen für das Vorhandensein der Sicherheitslücke

Die Hauptursachen für das Vorhandensein dieser Sicherheitslücke sind in der Regel unzureichende Kenntnisse in der Webserver-Konfiguration oder vernachlässigte Sicherheitsrichtlinien. Es ist wichtig zu betonen, dass alle etablierten Schwachstellenscanner diese spezifische Sicherheitslücke kostenfrei detektieren können, was die Vernachlässigung der regelmäßigen Schwachstellenprüfung noch gravierender macht.

Überprüfung der Schwachstelle

Die Existenz der Schwachstelle kann einfach überprüft werden, indem die URL des Datenverzeichnisses (`/data/`) im Webbrowser aufgerufen wird. Erhält man Zugang zu den Dateien, ist die Instanz verwundbar.

Zum Beispiel kann für eine Nextcloud-Instanz die folgende URL verwendet werden:

`http://cloud.example.org/data/nextcloud.log`

Für eine ownCloud-Instanz würde die URL entsprechend lauten:

`http://cloud.example.org/data/owncloud.log`

Handlungsempfehlung

Wurde eine verwundbare Instanz detektiert, so sollte die Webserver-Konfiguration schnellstmöglichst überprüft und angepasst werden, sodass der unauthentifizierte Zugriff auf sensible Daten und Verzeichnisse blockiert wird. Nach der Absicherung sollte das System auf Anzeichen von unberechtigtem Zugriff untersucht werden.

Ergebnisse der IT-Sicherheitsstudie

Die vorliegende Studie verdeutlicht das Ausmaß der Verwundbarkeit von ownCloud- und Nextcloud-Instanzen bezüglich der untersuchten Sicherheitslücke.
Die Ergebnisse sind alarmierend und werfen wichtige Fragen zur IT-Sicherheit und zum verantwortungsvollen Umgang bezüglich der regelmäßigen Sicherheitsüberprüfung von externen Unternehmensinfrastrukturen auf.

921
Millionen

Mit einem eigens entwickelten, hochperformanten Schwachstellenscanner wurden insgesamt über 921 Millionen Domains untersucht.

Dabei wurden nicht nur Domains der europäischen Länder, sondern auch über 655 Millionen Domains der .com Top Level Domain gescannt.

655
Millionen

9624
Instanzen

**Es wurden 9264 verwundbare Instanzen identifiziert, die ein breites Spektrum an Branchen betreffen.
Cyberkriminelle haben dadurch nicht nur Vollzugriff auf hochsensible Daten der betroffenen Organisationen, sondern auch auf die darin gespeicherten, sensiblen personenbezogenen Daten der jeweiligen Kunden.**

Lednerb / CloudPeeker

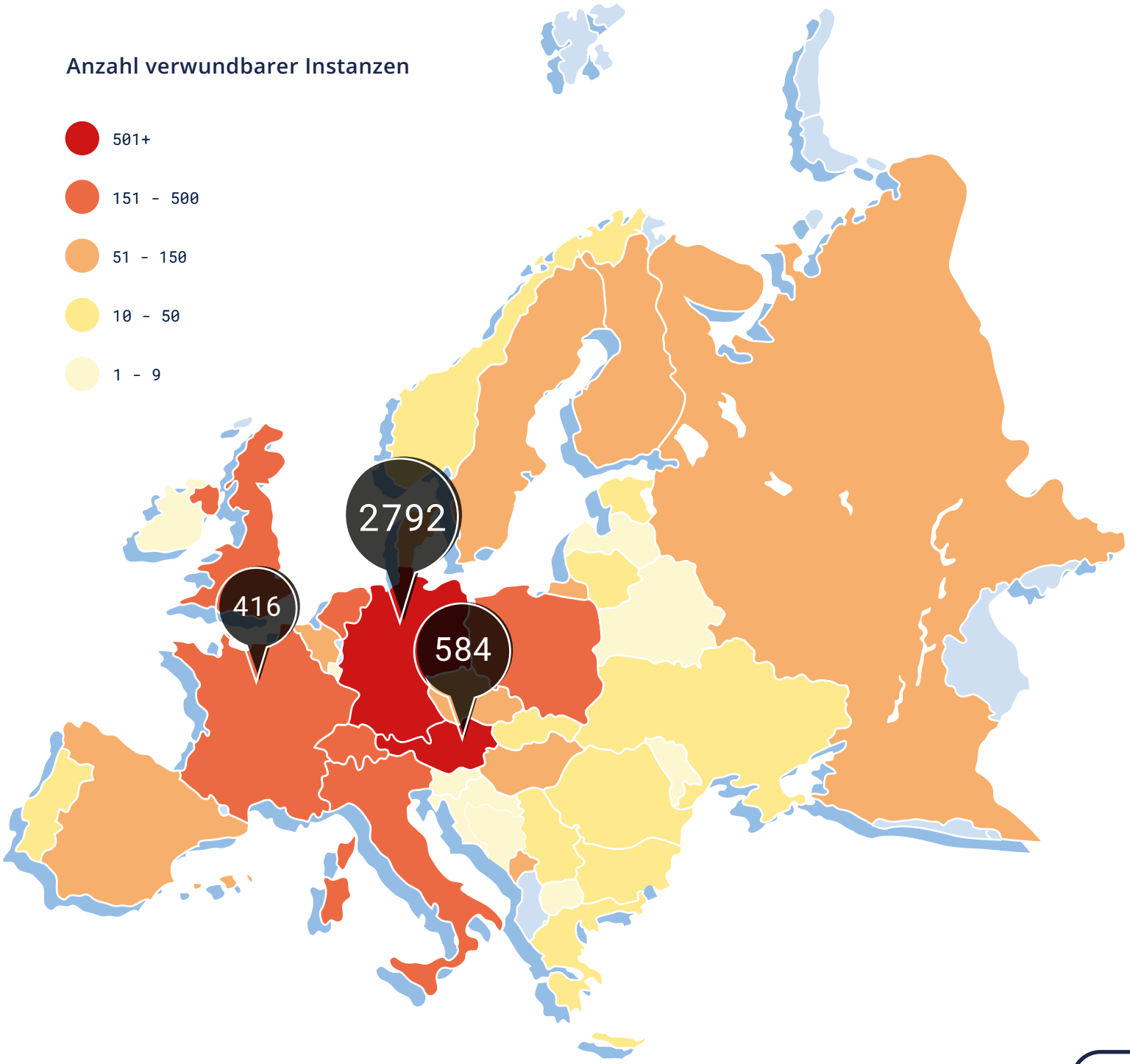
Unser eigens entwickelter, hochperformanter Scanner für die Sicherheitslücke « owncloud / Nextcloud Unprotected Data Directory » welcher unter einer Open Source Lizenz veröffentlicht wurde:

https://github.com/Lednerb/CloudPeeker

Verbreitung der Sicherheitslücke in Europa

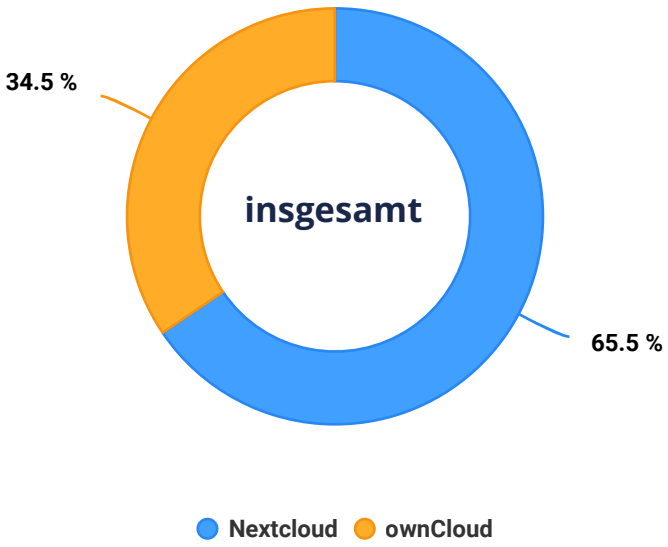
Unter den europäischen Top Level Domains wurden insgesamt 6954 betroffene Instanzen von ownCloud und Nextcloud identifiziert, wobei auffälligerweise über 50% dieser Fälle – nämlich 3595 Instanzen – im DACH-Raum lokalisiert sind. Die Verteilung dieser Instanzen in Europa zeigt eine deutliche Konzentration in bestimmten Ländern. Die Top 3 Länder mit den meisten betroffenen Instanzen sind Deutschland, Österreich und Frankreich.

6954
Instanzen



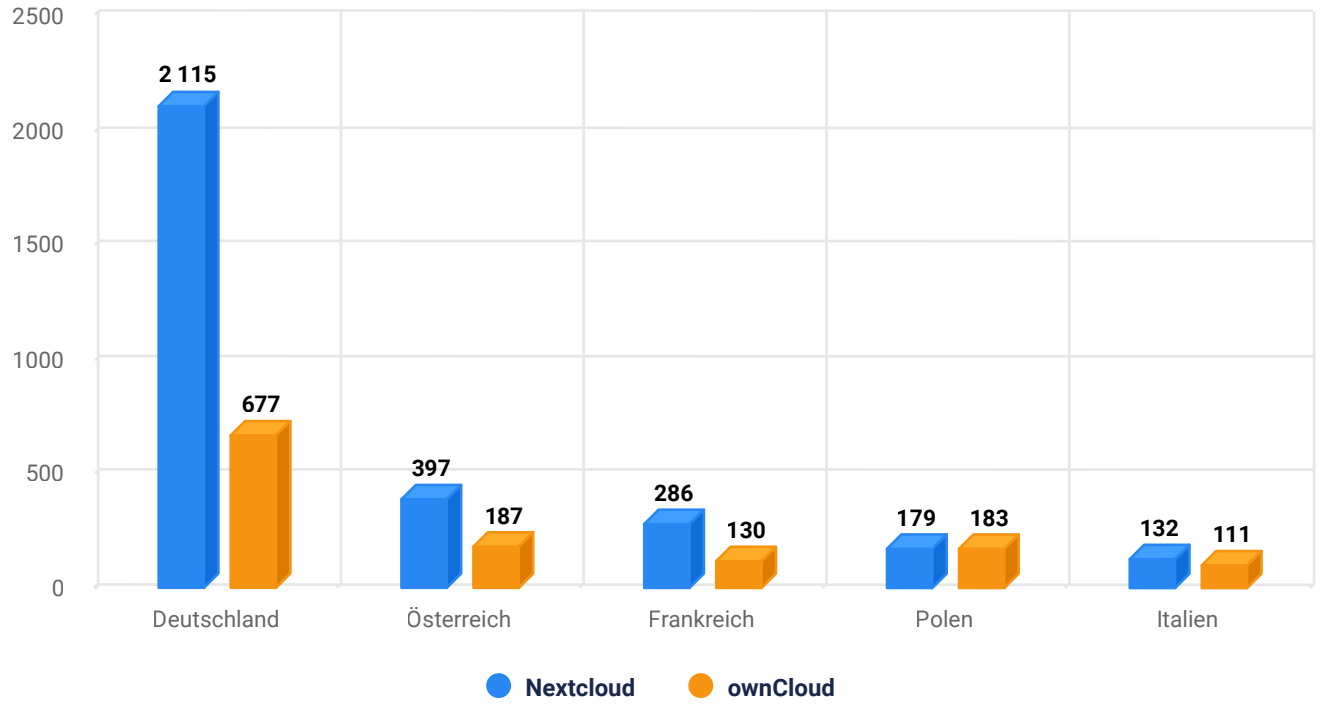
Verteilung verwundbarer ownCloud / Nextcloud Instanzen

Global betrachtet zeigt sich bei der Verteilung von verwundbaren Instanzen ein deutliches Übergewicht von Nextcloud, welche 65,5% der betroffenen Installationen ausmacht, verglichen mit 34,5% bei ownCloud. Diese Verteilung spiegelt sich auch in der Analyse spezifischer Länder wider, wobei signifikante Unterschiede in der Nutzung der beiden Cloud-Dienste erkennbar sind. Die europäische TLD (.eu) verzeichnet 579 verwundbare Instanzen mit einer Verteilung von 383 Nextcloud- zu 200 ownCloud-Instanzen.



Bei einem Vergleich der fünf Länder Deutschland, Österreich, Frankreich, Polen und Italien fällt auf, dass in den Datensätzen der verwundbaren Instanzen Nextcloud insgesamt häufiger auftritt als ownCloud. In Deutschland und Österreich, wo die meisten verwundbaren Instanzen identifiziert wurden, liegt der Anteil von Nextcloud-Instanzen deutlich höher als der von ownCloud. In Frankreich, Polen und Italien ist dieser Trend zwar ebenfalls erkennbar, jedoch mit einem geringeren Unterschied zwischen den beiden Anwendungen.

Aufteilung verwundbarer ownCloud- & Nextcloud-Instanzen



Betroffene Branchen & Unternehmen

Unter den detektierten 9624 verwundbaren Instanzen befinden sich zahlreiche private Nutzer, jedoch auch ein bedeutender Anteil von Unternehmen und Organisationen unterschiedlichster Größen und Branchen.

Zu den betroffenen Einrichtungen gehören Anwaltskanzleien, Krankenhäuser, Arztpraxen, Stromerzeuger und IT-Dienstleister. Auch öffentliche Verwaltungen, wie beispielsweise Städte und Gemeinden, und diverse Vereine gehören zu dem Kreis der Betroffenen. Die Schwachstelle betraf auch Datenschützer, deren Hauptverantwortung der Schutz sensibler Kundendaten ist.

Im privaten Bereich ermöglicht diese Sicherheitslücke den ungeschützten Zugriff auf persönliche Informationen wie Familienfotos, Finanzdaten, persönliche Dokumente und Bitcoin Wallets. Bei Unternehmen besteht ein hohes Risiko, dass sensible Informationen über Kunden oder Lieferanten, Patientendaten oder Zugänge zu Servern ungeschützt für Angreifer erreichbar sind.

Diese breite Palette an betroffenen Daten und Branchen zeigt die dringende

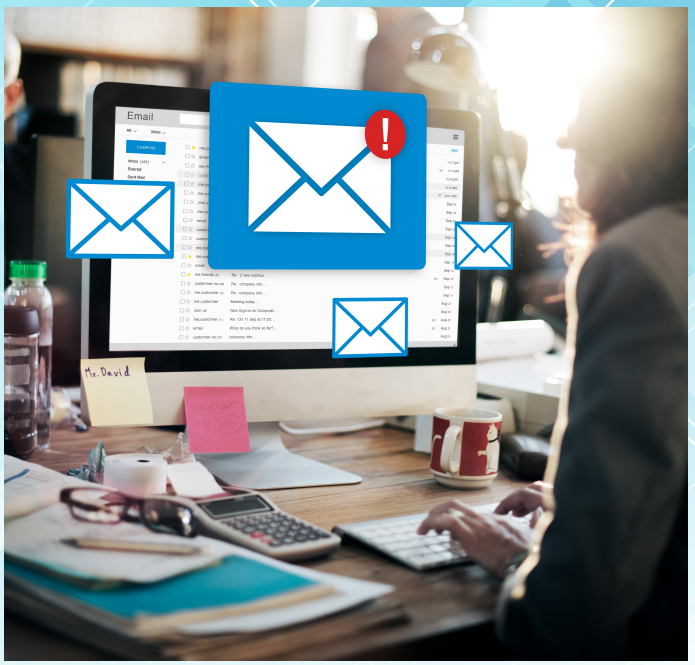
Notwendigkeit, Cybersicherheitsmaßnahmen über ein breites Spektrum von Anwendungsfällen hinweg zu verstärken.

Darüber hinaus waren auch Bildungseinrichtungen und Universitäten von dieser Sicherheitslücke betroffen, was den potenziellen Zugriff auf Forschungsdaten, Studenteninformationen und interne Dokumente ermöglicht. Dies wirft ernsthafte Bedenken bezüglich des Schutzes von geistigem Eigentum und sensiblen Forschungsdaten auf. Ebenso waren kleine und mittelständische Unternehmen betroffen, die oft nicht über die Ressourcen oder das Fachwissen verfügen, um ihre Systeme angemessen zu schützen. Dies macht sie zu einem besonders anfälligen Ziel für Cyberangriffe.

Zum Zeitpunkt der Veröffentlichung unserer Studie wurde festgestellt, dass der offizielle Nextcloud Security Scan *(`https://scan.nextcloud.com`)* die hier beleuchtete Schwachstelle nicht detektierte, obwohl deren Überprüfung relativ einfach möglich ist. Die Tatsache, dass ein wesentliches Werkzeug, welches von Nextcloud-Benutzern zur Überprüfung ihrer Systeme genutzt wird, diese spezifische Schwachstelle nicht erkennt, unterstreicht die Notwendigkeit für umfassendere und regelmäßige Sicherheitsüberprüfungen.

Erkenntnisse aus unserem Responsible Disclosure Verfahren

Im Zuge unseres Responsible Disclosure Verfahrens haben wir uns darauf konzentriert, betroffene Unternehmen zu kontaktieren, um sie über die kritische Sicherheitslücke in ihren ownCloud- und Nextcloud-Instanzen zu informieren. Dieser Ansatz wurde gewählt, da die Kontaktaufnahme mit Privatpersonen oft an fehlenden Kontaktinformationen scheiterte und die Auswirkungen eines Datendiebstahls bei Unternehmen, insbesondere in sensiblen Branchen wie bspw. dem Gesundheitswesen oder bei Rechtsanwälten, IT-Dienstleistern und Datenschützern, gravierender sind als bei Privatpersonen.



Unser erster Schritt in der Kontaktaufnahme war der Versuch, die jeweiligen Datenschutzbeauftragten der Unternehmen per E-Mail zu erreichen. Hierbei stellten wir mit Erstaunen fest, dass etwa 70% der `datenschutz`@-E-Mail-Adressen nicht funktionierten, da die Konten entweder voll waren oder schlicht nicht existierten. In Fällen, wo keine spezifischen Daten zum Datenschutzbeauftragten verfügbar waren, griffen wir auf allgemeine E-Mail-Adressen der Unternehmen zurück. Unsere E-Mails wurden größtenteils als Spam klassifiziert oder in der Flut der Nachrichten übersehen, was dazu führte, dass nur etwa 3-5 % der kontaktierten Unternehmen und Institutionen reagierten. Dies wurde durch eine spätere erneute Kontaktaufnahmen deutlich.

Bei telefonischen Versuchen, die richtigen Ansprechpartner zu erreichen, stießen wir häufig auf Herausforderungen. In vielen Fällen wurden wir nicht an die zuständigen Personen weitergeleitet und wurden des öfteren verbal angegriffen und beleidigt. Dennoch gab es auch positive Rückmeldungen von einigen Geschäftsführern und IT-Administratoren, die die Schwachstelle ernst nahmen und entsprechende Sicherheitsmaßnahmen einleiteten. Allerdings war dieser Prozess durch einen hohen Kosten- und Zeitaufwand geprägt.

In einem weiteren Experiment versandten wir an die 100 größten betroffenen Unternehmen und Institutionen einen detaillierten Sicherheitsbericht per Post.

Dieser enthielt ein Anschreiben, den Sicherheitsbericht mit Schwachstellenbeschreibung und Screenshots der offenliegenden Daten, sowie Handlungsempfehlungen zur Absicherung der Instanzen. Zusätzlich boten wir eine Log-File Analyse an, um ggf. feststellen zu können, ob die Sicherheitslücke bereits aktiv ausgenutzt wurde. Jedoch erhielten wir auf diese Postsendungen keinerlei Rückmeldungen. Eine erneute Überprüfung nach zwei Monaten zeigte jedoch, dass 53 der angeschriebenen Unternehmen die Sicherheitslücke behoben hatten.

Diese konkreten Erfahrungen verdeutlichen und bestätigen die Schwierigkeiten, denen White Hat Hacker und IT-Sicherheitsforscher begegnen, wenn sie versuchen, das Internet sicherer zu machen. Ihre Bemühungen, kritische Schwachstellen aufzudecken und zu melden, stoßen häufig auf Hindernisse, da ihre Kommunikation in einem Meer von Spam-Nachrichten und unaufgeforderten Verkaufsangeboten untergeht.

Unternehmen, die regelmäßig mit nicht verifizierten Sicherheitslücken konfrontiert werden, finden es oft herausfordernd, legitime Sicherheitswarnungen von irreführenden oder betrügerischen Kommunikationen zu unterscheiden. Diese Hindernisse führen zu einer unzureichenden Reaktion auf valide Sicherheitsmeldungen, was die Wichtigkeit von etablierten und effektiven Prozessen für das Schwachstellenmanagement und die Kommunikation über Cybersicherheitsbedrohungen in der Unternehmenswelt unterstreicht.

Es ist daher von entscheidender Bedeutung, das Bewusstsein für Cybersicherheit zu intensivieren und die Implementierung proaktiver Sicherheitsstrategien in allen Organisationstypen zu fördern, um eine robuste und resiliente digitale Infrastruktur zu gewährleisten.

Bereitstellung eines Kommunikationskanals im eigenen Unternehmen

Eine effektive Maßnahme, um von der weltweiten Cybersecurity-Community zu profitieren und die Sicherheit der eigenen IT-Infrastruktur zu stärken, ist die Implementierung einer `security.txt`-Datei.

Dieser einfache, aber wirkungsvolle Standard bietet einen klar definierten Weg für Sicherheitsforscher und White Hat Hacker, potenzielle Schwachstellen vertraulich zu melden. Informationen zur Implementierung dieses Standards finden sich unter `https://securitytxt.org`

Während die Einrichtung einer solchen Datei einen wichtigen Schritt darstellt, bringt sie auch Herausforderungen mit sich. Ein erhöhtes Aufkommen von Spam-Nachrichten und das Risiko, betrügerische oder schädliche „IT-Sicherheitsreports“ zu erhalten, sind real. Um diesen Herausforderungen zu begegnen und sicherzustellen, dass eingehende Meldungen sorgfältig geprüft und verarbeitet werden, bieten wir bei der Lednerb IT-Security GmbH eine spezialisierte Dienstleistung an. Diese zielt darauf ab, die Vorteile einer `security.txt`-Datei zu maximieren, während gleichzeitig die Risiken minimiert werden.

Unsere Dienstleistung:

Externer IT-Sicherheitskontakt

- ✔ Bereitstellung
- ✔ Filterung
- ✔ Analyse
- ✔ Verifikation
- ✔ Reporterstellung

LEDNERB

Weitere Informationen zu unserer Dienstleistung finden Sie auf unserer Website:

`https://lednerb.de/de/external-security-contact`

Lednerb IT-Security GmbH

+49 461 99 58 3448

https://lednerb.de

Lise-Meitner-Straße 2
24941 Flensburg

LEDNERB