

Sicherheitslücken, die Leben gefährden

Millionen Daten, Millionen Risiken

Datenlecks sind in unserer modernen, technisierten Welt leider keine Seltenheit, die möglichen Folgen sind bekannt: Sie schaden dem Ruf, schwächen die Cybersicherheit im Unternehmen, bei Verletzung der Vertraulichkeit oder der Integrität drohen hohe Bußgelder. Die Folgen können sich speziell im Bereich der kritischen Infrastruktur als schwerwiegend erweisen – Krankenhäuser sind hiervon nicht ausgenommen.

Im Februar 2024 wurde Change Healthcare, ein US-amerikanischer Anbieter im Gesundheitswesen, von der Ransomware-Gruppe BlackCat/ALPHV gehackt. Der initiale Zugriff erfolgte hier über öffentlich bekannte Zugangsdaten eines Support-Mitarbeiters für ein Citrix-Portal. Die Folgen: Gesundheitsdaten von mindestens 190 Millionen US-Amerikanern wurden gestohlen, darunter Krankenversicherungsinformationen, medizinische Aufzeichnungen, Abrechnungsdaten und in einigen Fällen sogar Sozialversicherungsnummern und Finanzdaten. Überdies dauerte es Monate, um den regulären Betrieb des Unternehmens nach erfolgreicher Verschlüsselung der Systeme durch die Angreifer wiederherzustellen – Angreifer, die im Nachgang 22 Millionen Dollar einkassiert haben, ohne die gestohlenen Daten wieder auszuliefern. Zusätzlich zu diesem Lösegeld beliefen sich die geschätzten Gesamtkosten des Angriffs, einschließlich Betriebsunterbrechungen und anderer finanzieller Auswirkungen, auf circa 2,5 Milliarden US-Dollar.^[1, 2] Dieses Beispiel zeigt eindrucksvoll, welche reale Bedrohung ein einziges öffentlich zugängliches Passwort eines Support-Mitarbeiters für den Gesundheitssektor darstellen kann.

Als Teil der kritischen Infrastruktur (KRITIS) waren Krankenhäuser noch vor wenigen Jahren für die meisten Cyberbedrohungsakteure tabu, die möglichen Folgen eines Ausfalls der Systeme oder deren Verschlüsselung waren auch damals schon bekannt. Doch die Lage ändert sich zusehends, denn spätestens seit dem russischen Angriffskrieg auf die Ukraine häufen sich Angriffe auf die kritische Infrastruktur – speziell innerhalb der Ukraine selbst, aber auch in unterstützenden NATO-Staaten – und somit auf Krankenhäuser. Ganz abgesehen von politisch motivierten Angriffen, können Kliniken ebenso ein profitables Ziel darstellen, da wohl allen Verantwortlichen daran gelegen sein dürfte, einen reibungslosen Betrieb zu gewährleisten und Daten von Patienten zu schützen; im Optimalfall, ohne negative Schlagzeilen zu erzeugen.

Bekannter Ansatz von Hackergruppen

Um ein Ziel wie ein Krankenhaus zu kompromittieren, benötigt ein Bedrohungsakteur (Threat Actor) in einem ersten Schritt einen initialen Zugang. Die meisten werden hier zu Recht an Phishing-E-Mails denken. Wir wollen in diesem Artikel aber gern einen anderen Angriffsvektor betrachten: Zugangsdaten von Klinikmitarbeitern, die im Internet und im Darknet für Hacker und Spezialisten zugänglich sind.

Aufgrund unserer Tätigkeit als Red Team und Targeted Threat Intelligence Provider verfügen wir über eine interne Datenbank, die aktuell knapp über 18 Milliarden geleakte oder im Untergrund verteilte Datensätze von Einzelpersonen beinhaltet. Die Daten wurden aggregiert, wobei der Schwerpunkt auf Benutzernamen und E-Mail-Adressen sowie den dazugehörigen Passwörtern lag. Zusätzlich angereichert durch langlebige Cookies in sogenannten „Stealer Logs“, die zum Beispiel in Azure-Umgebungen mehrere Wochen gültig sein können.

```
$ python3 NDBDB.py --query „*uniklinikum-<ZENSIERT>.de“  
<ZENSIERTE AUSGABE>  
[*] Found 1063 Results in 18.126.767.502 documents  
[*] Searching took 432 seconds
```

Zensierte, beispielhafte Anfrage an die interne Datenbank mit Anzahl der Ergebnisse

Name	Änderungsdatum	Typ	Größe
Applications	25.01.2025 17:14	Datenordner	
Online	25.01.2025 17:14	Datenordner	
Cookies	25.01.2025 17:14	Datenordner	
Edge	25.01.2025 17:14	Datenordner	
GoogleAccounts	25.01.2025 17:14	Datenordner	
Notes	25.01.2025 17:14	Datenordner	
All Passwords.txt	25.01.2025 17:14	TXT-Datensatz	5 KB
BitLocker.txt	25.01.2025 17:14	TXT-Datensatz	1 KB
Clipboard.txt	25.01.2025 17:14	TXT-Datensatz	1 KB
Processes.txt	25.01.2025 17:14	TXT-Datensatz	4 KB
Software.txt	25.01.2025 17:14	TXT-Datensatz	3 KB
System.txt	25.01.2025 08:59	TXT-Datensatz	2 KB

```
(ndb) python3 search.py -q "uniklinik.***.*** -f oneline -fds en,url  
...  
[*] Querying Index ***.com ...  
[*] Querying Index ***.de ...  
[*] Querying Index ***.ch ...  
[*] Found 688 results in 18126767502 documents  
[*] Searching took 147.3128383159637 seconds
```

Gestohlene Zugangsdaten einer deutschen Klinik (Bild: NSIDE)

Um zu testen, wie groß die potenzielle Angriffsfläche für einen initialen Zugang und die Möglichkeit der Fortbewegung nach der ersten Kompromittierung im Netzwerk ist, wurde eine Liste von Kliniken gegen unsere interne Datenbank geprüft – mit erschreckendem Ergebnis.

Analyse der gefundenen Daten

Im Rahmen unserer Untersuchung zur Sicherheit von Zugangsdaten im Gesundheitssektor wurde eine Stichprobe von circa 2.600 Domains analysiert, die Krankenhäusern weltweit zugeordnet sind. Diese wurden ausgewählt, da sie zu den besonders sensiblen Bereichen dieser ohnehin zur kritischen Infrastruktur zählenden Branche gehören. Die ausgewerteten Daten stehen dabei exemplarisch für den Gesundheitssektor.

Die Ergebnisse unserer Analyse sind alarmierend: Insgesamt wurden 745 unterschiedliche Domains identifiziert, bei denen mindestens ein Treffer vorlag. Der gefilterte Datensatz enthält rund 250.000 Zugangsdaten zu Benutzerkonten, die in Verbindung mit der jeweiligen Domain stehen. Davon konnten mehr als 9.000 Einträge 39 Domains deutscher Kliniken zugeordnet werden – allein ein großes deutsches Krankenhaus ist mit über 2.000 kompromittierten Datensätzen betroffen.

Auch wenn die gefundenen Passwörter oder Cookies nicht zwangsläufig dem betroffenen Klinik-Account zugerechnet werden können, stellen sie potenziell ein erhebliches Sicherheitsrisiko dar, da diese Konten zumindest auf kompromittierten Geräten genutzt wurden. Dadurch könnte ein Angreifer ein indirektes Einfallstor erhalten.

Zusätzlich zur Domainanalyse haben die Experten die Qualität der Passwörter untersucht. Dabei zeigte sich eine weitere Schwachstelle: Mit einer durchschnittlichen Passwörterlänge von nur acht Zeichen bei einer mittleren Entropie von 41,36 Bits liegen diese Werte unterhalb des empfohlenen Sicherheitsstandards.^[3, 4] Zudem wurden über 38.000 Passwörter mehrfach verwendet, was auf eine hohe Wiederverwendungsrate hinweist. Ein Abgleich mit drei gängigen Passwort-Wörterlisten^[5] ergab, dass rund 95.000 der analysierten Passwörter in mindestens einer dieser Listen vorhanden sind.

Die Analyse der Daten legt nahe, dass häufig private Geräte für den dienstlichen Zugang genutzt werden oder umgekehrt. Möglich ist auch die Nutzung kompromittierter Endgeräte durch mehrere Personen, beispielsweise in gemeinsam genutzten Behandlungsräumen. Die Analyse zeigt zudem, dass bei der Passwortstärke noch erheblicher Verbesserungsbedarf besteht.

Empfehlungen

Insgesamt verdeutlicht die Untersuchung die bestehenden Schwachstellen und zeigt, wie dringend Maßnahmen zur Verbesserung der Cybersicherheit im Gesundheitssektor erforderlich sind. Um die Risiken zu minimieren und den Schutz sensibler Patientendaten zu gewährleisten, sind gezielte Sicherheitsvorkehrungen notwendig, zum Beispiel:

- **Sicherheitsbewusstsein stärken:**
 - Jeder Mitarbeiter ist ein potenzielles Ziel für Angreifer.
- **Angriffsvektoren minimieren:**
 - Identifikation und Reduzierung potenzieller Einfallstore, zum Beispiel durch Sicherheitsprüfungen und Härtung von Systemen
 - Begrenzung von Zugriffsrechten (Least Privilege Principle)
 - klare Richtlinien für private und dienstliche Geräte (BYOD)
 - Härtung gemeinsam genutzter Geräte durch eingeschränkte Konten und Systemprüfungen
- **Schutz kompromittierter Zugangsdaten:**
 - regelmäßige Überprüfung, ob Zugangsdaten in bekannten Datenlecks auftauchen
 - Umsetzung von Maßnahmen wie automatische Sperrlisten oder erzwungene Passwortänderungen bei Verdacht auf Kompromittierung
- **Awareness-Trainings und Notfallübungen:**
 - regelmäßige Awareness-Schulungen und simulierte Angriffe zur praxisnahen Sensibilisierung der Mitarbeiter
 - Etablierung von klaren Meldewegen für Sicherheitsvorfälle
- **Adaption bewährter Sicherheits-Frameworks^[6]:**
 - TIBER: Durchführung gezielter Red-Teaming-Tests zur Identifikation realer Schwachstellen
 - DORA: Umsetzung robuster Prozesse zur digitalen Resilienz und kontinuierlichen Verbesserung der IT-Sicherheit
- **Cybersicherheit als fortlaufenden Prozess begreifen:**
 - Schutzmaßnahmen regelmäßig evaluieren und anpassen
 - IT-Sicherheit in der Unternehmenskultur verankern ■

Literatur

- ^[1] HIPAA Journal. Change Healthcare Responding to Cyberattack. www.hipaajournal.com/change-healthcare-responding-to-cyberattack/
- ^[2] Hyperproof. Understanding the Change Healthcare Breach. <https://hyperproof.io/resource/understanding-the-change-healthcare-breach>
- ^[3] National Institute of Standards and Technology (NIST). Digital Identity Guidelines: Authentication and Lifecycle Management, Special Publication 800-63B, 2017. <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-63b.pdf>
- ^[4] Bundesamt für Sicherheit in der Informationstechnik (BSI). Sichere Passwörter erstellen. www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html
- ^[5] Daniel Miessler. SecLists – Security Testers Companion. <https://github.com/danielmiessler/SecLists>
- ^[6] NSIDE ATTACK LOGIC. Was ist Targeted Threat Intelligence (TTI)? www.nsideattacklogic.de/was-ist-targeted-threat-intelligence-tti/



Anna Dilber

ist IT Security Analyst
bei NSIDE ATTACK LOGIC.



Fabian Diener

ist IT Security Analyst
bei NSIDE ATTACK LOGIC.