CCVOSSEL

We know IT.

SUCCESS STORY

Medizintechnik Rostock GmbH | CCVOSSEL

Penetrationstest

Bild: Shutterstock / Mikko Lemola

Anforderungen

Um ein vollumfängliches Bild über den aktuellen Stand der firmeneigenen IT-Sicherheit zu erhalten und diese zu verbessern, beauftragte die Medizintechnik Rostock GmbH (MTR) die CCVOSSEL GmbH mit einem Penetrationstest.

Gemeinsam mit den Verantwortlichen der MTR wurden im Vorfeld bestimmte Sicherheitsmechanismen definiert, die den Netzwerkbetrieb während der Durchführung des Penetrationstests gewährleisteten. Wichtige Server und Systeme, die zur Aufrechterhaltung der Netzwerkbestandteile und deren Funktionen essenziell sind, wurden entsprechend identifiziert.

Im Rahmen des Penetrationstests sollte die gesamte IT-Infrastruktur des Unternehmens sowohl von außen als auch von innen (Assume Breach) getestet werden. Hierbei galt es insbesondere zu berücksichtigen, dass beispielsweise eigene Mitarbeiter (un)absichtlich Angriffe auf die IT-Infrastruktur des Unternehmens in der Realität ausführen bzw. auslösen können. Ebenfalls wünschte sich der Kunde eine Analyse des Active Directory auf mögliche Fehlkonfigurationen und Angriffswege sowie eine Überprüfung der bestehenden Berechtigungskonfigurationen und aller Dokumente auf Netzwerkfreigaben.

Umsetzung

Die Entscheidungsträger der MTR legten ein besonderes Augenmerk auf eine vertrauensvolle Zusammenarbeit. Aus diesem Grund war es ihnen wichtig, die Kick-Off Veranstaltung vor Ort durchzuführen. Es wurde ein Zeitfenster für die Durchführung des Penetrationstests festgelegt und weitere Informationen, wie z.B. von der Sicherheitsüberprüfung betroffene IP-Adressen und URLs final in der sogenannten Permission-To-Attack (Angriffsgenehmigung) dokumentiert. Diese muss zwingend vom jeweiligen Daten- und Hardwareeigner der zu testenden Systeme vorab bestätigt und unterzeichnet werden.

Als nächster Schritt erfolgte das Einbetten der Analysebox im Unternehmensnetzwerk der MTR. Bei der Analysebox handelt es sich um eine Computerkomponente, die den verantwortlichen CCVOSSEL-Pentestern den Zugriff sowie die Steuerung via LTE ermöglicht. Somit konnte die Durchführung des Penetrationstests remote erfolgen, wodurch die Flexibilität aller beteiligten Personen gesteigert und anfallende Kosten gesenkt werden konnten.

Nach Abschluss der Planung erfolgte die erste Scanphase. Durch bereits vorher definierte Scanparameter konnte diese innerhalb eines kurzen Zeitraums halbautomatisiert vonstatten gehen. Hierbei werden unter anderem Ports gescannt, Protokolle und laufende Versionen registriert sowie der Netzwerkverkehr und Konfigurationen überprüft. Dabei kann ein gegebenenfalls unverschlüsselter Netzwerkverkehr eine besondere Art der Bedrohung darstellen. Im konkreten Fall der MTR konnten die Experten der CCVOSSEL GmbH den Kunden auf Fehlkonfigurationen der Telekommunikationseinrichtungen hinweisen.

Nach Bekanntwerden dieser Informationen gab es dank guter Kommunikation ein unmittelbares Meeting, welches zu einer schnellen Behebung der Schwachstelle führte.

Vor der Tiefenanalyse, in der untersucht wird, wie ein Angreifer vom Punkt des Eintretens in ein System weiterkommen und möglicherweise Schaden anrichten kann, sichteten die Pentester die Ergebnisse der ersten Scanphase. Basierend darauf wurde eine Priorisierung zur weiteren Vorgehensweise erarbeitet, wobei sowohl die Kritikalität des Systems als auch der gescannten Schwachstellen ausschlaggebend war.

Unter Abwägung der Risiken richteten sich die geplanten Angriffe im Anschluss zunächst auf Systeme von Mitarbeitern, welche nicht in der IT-Abteilung beschäftigt waren. Ebenfalls standen Peripheriegeräte wie Drucker oder Switches im Zentrum der Aufmerksamkeit, da für diese oftmals Standardpasswörter genutzt werden. In diesem Kontext ist vor allem auf die Möglichkeit potenzieller DSGVO-Verstöße zu verweisen.

Bei der simultan stattfindenden Fehlerkonfigurationsanalyse des Active Directory war es den Pentestern, durch die manuelle Ausnutzung einer Schwachstelle, möglich Server des Kunden ein- und auszuschalten.

Weiterhin konnte das Ziel die Domäne zu übernehmen ebenfalls erreicht werden. Dadurch wäre im Ernstfall das Fortsetzen des Geschäftsbetriebes gefährdet gewesen.

Fazit & Ausblick

Der Penetrationstest wurde mit einer umfassenden Dokumentation abgeschlossen, welche in Form eines ausführlichen Abschlussberichtes an die MTR übergeben wurde. Dieser enthält neben einer Auflistung aller Findings auch Empfehlungen, wie identifizierte Schwachstellen behoben werden können. Weiterhin wurden alle Angriffe – unabhängig von deren Ergebnis – mit einem jeweiligen Proof of Concept dokumentiert.

In einer abschließenden Management Präsentation wurden die kritischen Schwachstellen erläutert und deren potenzielle Folgen für den Geschäftsbetrieb dargestellt.

Um vom Know-How der CCVOSSEL zu profitieren und die Angriffsvektoren so schnell wie möglich zu beseitigen, wurde die Behebung kritischer Findings als Folgeauftrag an CCVOSSEL übergeben. Die gegenseitige Wertschätzung sowie das entgegengebrachte Vertrauen während der gesamten Zeit der Zusammenarbeit spielte dabei eine wesentliche Rolle. Auf diesem Wege konnte die Sicherheit der MTR entscheidend gesteigert und optimiert werden.

CCVOSSEL

We know IT.

Sicherheit

360° Überprüfung und
Optimierung Ihrer IT-Sicherheit

Business Solutions

Professionelle IT-Services
rund um Ihre Infrastruktur

Softwareentwicklung

Optimierung Ihrer Prozesse
durch angepasste Lösungen

CCVOSSEL steht seit über 25 Jahren für professionelle IT-Dienstleistungen

Wir engagieren uns für unsere Kunden und für eine offene Gesellschaft. Unser Fokus liegt dabei in der Absicherung und dem Betrieb von IT-Systemen mit dem Schwerpunkt IT-Sicherheit. Durch den Einsatz interdisziplinärer Teams bestehend aus Administratoren, Beratern, Datenanalysten und Softwareentwicklern ermöglichen wir auch bei komplexen Anforderungen effiziente und moderne Lösungen.

Unsere Kunden

Siemens Bosch Daimler AG
Lufthansa System Network GmbH
Howoge Servicegesellschaft mbH
John F. Kennedy Friendship Center e.V.
Vattenfall Deutsche Bank AG
Gilette Deutschland GmbH & Co. OHG
BMW KPMG Agilent Technologies
Trägerverein des deutschen Presserats e.V.
Sony Europe GmbH G + J Berliner Verlag GmbH
Roche

Kooperationen

Microsoft Partner
Microsoft
Gold Application Development
Gold Datacenter
Silver Messaging

it's.BB
DAS IT-SICHERHEITSNETZWERK BERLIN-BRANDENBURG

SecurITy made in Germany

Allianz für Cyber-Sicherheit

Zertifizierungen

ISO/IEC 27001 zertifiziert www.isocert.de

ISO 9001 zertifiziert www.isocert.de

CCVOSSEL GmbH

www.ccvossel.de | info@ccvossel.de | FreeCall: 0800 2286773 | + 49 30 6098409 – 0

Standort Berlin Prenzlauer Berg | Sredzkistraße 28 | 10435 Berlin

Standort Berlin Tempelhof | Rathausstrasse 48 | 12105 Berlin