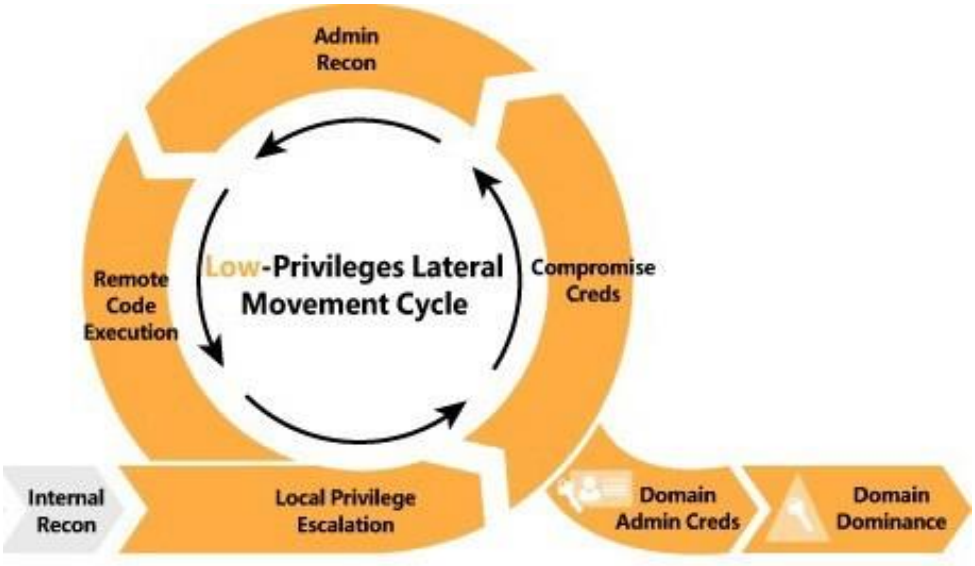
Penetrationstest für Active Directory

Active Directory ist ein Verzeichnisdienst, der von Microsoft für das Windows-Domänennetzwerk entwickelt wurde. Innerhalb von IT-Infrastrukturen von Unternehmen wird der Dienst meist zur Verwaltung von Benutzern und Computern mit einem einzigen Kontrollpunkt, dem „Domänen-Controller“, verwendet. Über 90 % der umsatzstärksten Unternehmen der Welt setzen beim wirksamen Management ihrer Ressourcen auf Active Directory. Bei einem Penetrationstest für Active Directory in einer Windows-Umgebung wird ein Angriff per Zugang zum Unternehmensnetzwerk simuliert. Dieser Zugang kann physisch oder über einen infizierten Arbeitsplatzrechner erfolgen. Vorrangig geht es darum, anfällige Assets in der Sicherheitszone des Unternehmens zu finden und Vorschläge zur Optimierung der Sicherheit von Active Directory zu machen. Das Ziel des Penetrationstests für Active Directory ist die Identifizierung von Schwachstellen im internen Unternehmensnetzwerk.



Leistungsumfang

Der Kunde legt den Umfang des Penetrationstests für Active Directory fest und stellt einen VPN-Zugang zu seinem internen Netzwerk zur Verfügung. Dieser Penetrationstest wird über Remote-VPN innerhalb des betreffenden Unternehmens durchgeführt. Ziel ist in der Regel die Identifizierung und Klassifizierung von Bedrohungen und Schwachstellen im internen Netzwerk, die auf einen bereits bestehen- den Zugang zum Unternehmensnetzwerk, beispielsweise durch einen Mitarbeiter, Auftragnehmer oder Gast, zurückzuführen sind. Unsere Penetrationstests umfassen Sicherheitsprüfungen, die dazu dienen, negative Auswirkungen auf die Produktionsumgebung des Unternehmens zu begrenzen.

Prozess des Penetrationstests für Active Directory

- **Interne Reconnaissance:** Ausgangspunkt sind die Zugangsrechte des Standardbenutzers. Ziel ist das Aufspüren lokaler Schwachstellen im System, die ausgenutzt werden können, um Zugangsrechte lokaler Administratoren zu erlangen. In dieser Phase werden Informationen über die Active-Directory-Infrastruktur mittels eines Zugangs für nicht zugangsberechtigte Benutzer gesammelt.
- **Administrator-Reconnaissance**: Ist die Enumeration mit dem Standardbenutzer beschränkt, können Administrator Zugangsdaten für die weiteren Schritte der Reconnaissance verwendet werden.
- **Identifizierung der Schwachstellen:** Basierend auf den in den vorherigen beiden Phasen gesammelten Informationen identifizieren wir schwache Dienste in Ihrem Netzwerk oder Anwendungen mit bekannten Schwachstellen.
- **Exploitation:** Wir nutzen bereits verfügbaren Code oder erstellen einen benutzerdefinierten Code, um die identifizierten Schwachstellen zu nutzen und Zugang zu dem betreffenden anfälligen System zu erhalten.
- **Eskalation der Zugangsrechte:** In einigen Fällen bietet die bestehende Schwachstelle nur Zugang auf einer einfachen Ebene, etwa dem normalen Benutzerzugang mit beschränkten Zugangsrechten. In diesem Schritt versuchen wir, einen Zugang mit vollständigen Administratorrechten zu diesem Gerät zu erhalten.
- **Zugangsdaten eines Domänen-Administrators:** Mittels des Zugangs als Domänen-Administrator wird versucht, die Gesamtstruktur-Stammdomäne zu manipulieren und damit das gesamte Active-Directory- Netzwerk des Unternehmens zu beherrschen.

Kontakt

Wenn Sie mehr über Penetrationstest für Active Director erfahren möchten, kontaktieren Sie uns doch gerne.

Sie erreichen uns, Ihren Partner für IT-Support, telefonisch von Montag bis Freitag zwischen 9 und 18 Uhr. Natürlich können Sie uns jederzeit eine E-Mail schreiben oder eine Nachricht über das Kontaktformular senden. Wir freuen uns, von Ihnen zu hören und sind gespannt, welches Projekt bei Ihnen ansteht.

Lilienthalstraße 3, 82178 Puchheim	Mail: info@albitc.de	Telefon: 089/36055272