c-ray.solutions

Office 365 Sicherheitsüberprüfung
für
C-Ray

Datum: 12.07.2023

Vielen Dank!

Dafür, dass Sie die Beta-Version von C-Ray getestet haben.

Wir hoffen, der folgende Bericht hilft Ihnen Ihre Office-365 und Azure Umgebung besser zu verstehen und diese abzusichern.

Da es sich um eine Beta-Version handelt, ist es möglich, dass noch Fehler jeglicher Art im Bericht zu finden sind. Sollte Ihnen etwas auffallen oder unklar sein, sind wir sehr dankbar über Ihre Rückmeldung. Natürlich freuen wir uns auch auf jede andere Art von Nachricht. Zum Beispiel wie Ihnen das Programm, der Bericht und die Anwendung gefällt oder welche Kritik Sie daran haben. Ganz einfach per Mail an info@c-ray.solutions.

Wir freuen uns von Ihnen zu hören
Ihr C-Ray-Team

P.S.: Vergessen Sie bitte nicht, den Report bei sich zu speichern, am Ende der Beta-Phase werden alle Konten zurückgesetzt. Alle Angaben sind ohne Gewähr.

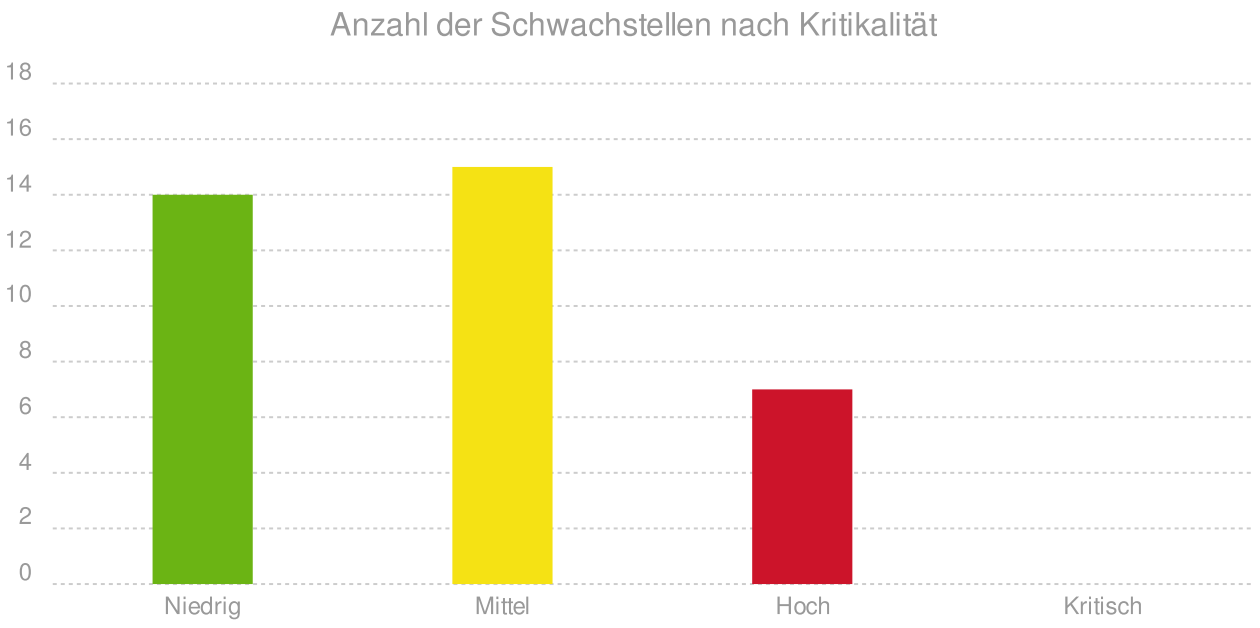
Inhaltsverzeichnis

Executive Summary

Am 12.07.2023 hat C-Ray eine vollständig automatisierte Überprüfung des Azure Active Direcotry "C-Ray" und dem zugehörigen Exchange Online vorgenommen. Dabei wurden sämtliche Sicherheitseinstellungen, welche unter den abonnierten Lizenzen zur Verfügung stehen, überprüft. Jegliche sicherheitsrelevante Abweichung von Empfehlungen ist inklusive einer detaillierten Beschreibung, dem ermittelten Risiko und geschätztem Behebungsaufwand, sowie einer detaillierten Anleitung zur Anpassung in diesem Bericht ausgeführt.

Sollten Sie Fragen zu den Ergebnissen haben, einen zur Weitergabe vorgesehenen Bericht wünschen oder Unterstützung bei der Umsetzung der Empfehlungen suchen, helfen wir Ihnen gerne. Kontaktieren Sie uns dazu bitte per Mail an info@C-Ray.solutions.

Im Zuge der Überprüfung wurde festgestellt, dass 14 Schwachstellen mit niedrigem Risiko, 15 Schwachstellen mit mittlerem Risiko, 7 Schwachstellen mit hohem Risiko und keine kritische Schwachstellen in Ihrer Umgebung existieren. Die Verteilung ist daher wie nachfolgend abgebildet.



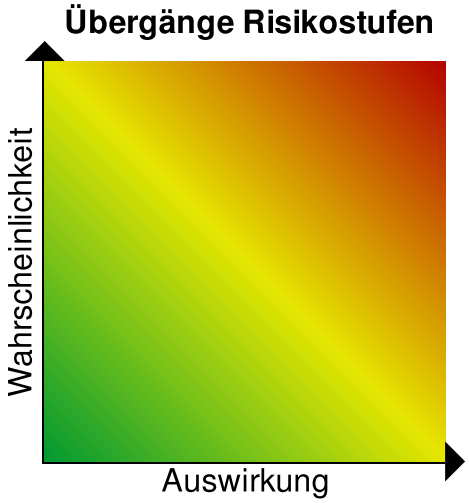
Umfang und Methodik

Im Zuge der Überprüfung wurde Ihr Azure Active Directory sowie (falls vorhanden) Exchange Online auf die Implementierung aktueller Sicherheitsempfehlungen überprüft.

Die Überprüfung berücksichtigt Ihre aktuell gewählte Lizenz für Azure Active Directory sowie Exchange Online. Aktuell stellt Microsoft eine kostenlose, Premium 1 und Premium 2 Lizenz zur Auswahl zur Verfügung. Jede der Premium Lizenzen bietet weitere Anpassungsmöglichkeiten, wobei Premium 2 die meisten Möglichkeiten bietet, aber auch zum höchsten Preis pro Benutzer kommt. Wichtig ist, dass bei Umsetzung der Empfehlung unabhängig von der gewählten Lizenz eine sehr hohes Schutzniveau erreicht werden kann.

Risikoevaluierung

C-Ray unterscheidet zwischen den vier Risikoabstufungen Niedrig, Mittel, Hoch und Kritisch. Für die jeweiligen Stufen gilt nachfolgende Definition. Beachten Sie jedoch, dass nicht jedes Szenario in diesen Abstufungen berücksichtigt werden kann und die Übergänge zwischen den Stufen fließend sind.



Diese Übergänge werden durch nebenstehende Grafik veranschaulicht. Beachten Sie, dass es sich bei Risiko immer um das Verhältnis der Auswirkung zur Eintrittswahrscheinlichkeit handelt. Es resultiert also aus großer Eintrittswahrscheinlichkeit und hoher zu erwartender Auswikrung bei Eintritt ein hohes Risiko.

Niedrig

Diese Empfehlungen gehen über die aktuell empfohlenen Sicherheitseinstellungen hinaus. Viele davon vereinfachen bei einem erfolgten Angriff die Aufarbeitung, tragen aber nicht dazu bei diesen zu verhindern. Außerdem finden sich hier auch Empfehlungen, die möglicherweise unbeabsichtigte Aktionen erschweren. Ein Beispiel für letzteres ist die gängige Nachfrage "Sind Sie sicher, dass sie dieses Objekt Löschen möchten?" nachdem bereits auf löschen geklickt wurde.

Mittel

Wenn diese Empfehlungen nicht umgesetzt werden steigt die Wahrscheinlichkeit von Aktionen, die mit einer Einschränkung der Verfügbarkeit, Vertraulichkeit oder Integrität Ihrer Systeme oder Daten einhergehen. Diese Aktionen lassen sich entweder ohne Einschränkungen schnell rückgängig machen oder haben einen zeitlich begrenzten Einfluss (zum Beispiel durch Angriffe, die auf Systemüberlastungen abzielen). Im Falle eines Datenabflusses ist dieser im Umfang begrenzt (z.B. nur jene Daten auf die ein bestimmter Benutzer Zugriff hat).

In diese Kategorie fallen außerdem erweiterte Schutzmaßnahmen für normale Benutzerkonten.

Hoch

Empfehlungen dieser Stufe sind grundlegende Sicherheitseinstellungen, die unbedingt in jeder Umgebung vorhanden sein sollten. Wenn diese Empfehlunge nicht umgesetzt werden steigt die Wahrscheinlichkeit von Aktionen, die mit einer erweiterten Einschränkung der Verfügbarkeit, Vertraulichkeit oder Integrität Ihrer Systeme oder Daten einhergehen stark.

Diese Aktionen lassen sich entweder nicht (z.B. Datenverlust ohne Backup) oder nur sehr aufwendig (z.b. Wiederaufbau der Netzwerkumgebung, Verlust des Zugangs zur Umgebung) rückgängig machen. Außerdem finden sich hier Empfehlungen, welche die Auswirkungen eines Datenverlustes begrenzen (statt sämtlicher Unternehmensdaten z.B. nur die Daten eines Systems).

In dieser Kategorie finden sich außerdem grundlegende Schutzmaßnahmen für sämtliche Benutzerkonten, sowie erweiterte Empfehlungen für den Schutz von Administratoren.

Kritisch

In diese Kategorie fallen sämtliche Aktionen, die ohne ein Benutzerkonto, jederzeit und über das Internet ausgeführt werden können, also eine unmittelbare Gefahr darstellen (z.B. Zugang zu Verwaltungsschnittstellen über das Internet die keine Anmeldung erfordern). Darüber hinaus finden sich hier Empfehlungen, die, falls nicht umgesetzt, in vielen Fällen existenzgefährdenden Einfluss auf Ihr Unternehmen haben können.

Außerdem fallen in diese Kategorie grundlegende Schutzmaßnahmen für Administratoren wie die Mehrfaktorauthentifizierung.

Aufwand

C-Ray bietet Ihnen zu jeder identifizierten Schwachstelle eine Einschätzung des technischen Behebungsaufwands. Da unternehmensinterne Planungs-, Abstimmungs- und Kommunikationsmaßnahmen je nach Unternehmen und Umgebung sehr stark variieren, können diese nicht seriös berücksichtigt werden.

Die Abstufung des Behebungsaufwands erfolgt in den drei Stufen Niedrig, Mittel und Hoch, welche wie folgt definiert sind:

Niedrig
Hierbei handelt es sich um Maßnahmen, die sehr schnell umgesetzt werden können, wenig bis keine technische Planung erfordern, keinen oder nur einen sehr kurzzeitigen Testbetrieb benötigen und keine fortlaufenden Aufwände verursachen.

Beispiele hierfür sind das Anbinden weiterer Systeme an ein vorhandenes System zur Aufbewahrung von Logdaten, das Löschen von Ressourcen die nicht mehr in Verwendung sind sowie das Aktualisieren von Passwörtern, die nur von Systemen und nicht Personen verwendet werden.

Mittel
Hierbei handelt es sich um Maßnahmen, die komplexer in der Umsetzung sind, genauere technische Planung erfordern, einen ausführlicheren Testbetrieb benötigen oder zumindest nach der Umsetzung einen zeitlich begrenzten wiederkehrenden Aufwand verursachen.

Beispiele hierfür sind das Aktivieren der Mehrfaktorauthentifizierung für Benutzer oder das Konfigurieren einer Firewall, die Webanwendungen schützt (eine sogenannte Web Application Firewall, kurz WAF). Ersteres erfordert eine genaue Planung und in der Regel nach der Umsetzung geringen, aber stetigen Betreuungsaufwand der Benutzer, während die WAF erst nach einer ausführlichen Testphase aktiviert werden sollte.

Hoch
Diese Maßnahmen erfordern die genaueste Planung, einen ausgiebigen Testbetrieb, erheblich Zeit in der Umsetzung oder verursachen größeren, fortlaufenden Aufwand im Betrieb.

Beispiele für Maßnahmen mit hohem Aufwand sind das Ausrollen eines neuen Betriebssystems oder -version im gesamten Unternehmen (Planung und Testbetrieb), eine weitgehende Anpassung der Netzwerkarchitektur (Planung und Umsetzung) oder Installation und Betrieb eines Backupsystems.

Benutzer ohne Administratorrolle können Sicherheitsgruppen erstellen

Risiko	Hoch	Aufwand	Niedrig

Beschreibung

Sicherheitsgruppen werden in Azure Active Directory verwendet, um Personen in Gruppen zu organisieren, die Gemeinsamkeiten wie z.B. die Abteilung, den Firmenstandort oder ähnliches teilen. Diesen Gruppen werden anschließend Rechte zugewiesen.

Ein Angreifer hat folgende Möglichkeit diese Fähigkeit zu missbrauchen, die als äußerst gefährlich erachtet werden muss. Erstellt ein Angreifer über 2048 Gruppen und fügt sämtliche Benutzer in Ihrer Umgebung als Mitglieder hinzu, so besteht die Gefahr, dass sich keiner dieser Benutzer mehr anmelden kann und Ihr Zugriff auf den Tenant verloren geht. Die Erwähnung dieses Verhaltens seitens Microsoft ist in den Referenzen verlinkt.

Darüber hinaus besteht die Gefahr, dass Benutzer mehrere Gruppen erstellen, welche dieselben Personen beinhalten und für denselben Zweck verwendet werden. Angenommen es gibt eine Gruppe Marketing die von Benutzern erstellt wurde und eine Gruppe Werbung die von den Administratoren erstellt wurde. Beide Gruppen beinhalten die gesamte Marketingabteilung und sonst niemanden. So kann es passieren, dass beiden Zugriff auf die Daten zur nächsten Kampagne gegeben wird. Wechselt nun eine Person aus dem Marketing in den Versand und wird nur aus der Gruppe Werbung entfernt, nicht aber aus der Gruppe Marketing, kommt es zu einer Mitnahme von Rechten, die die Person in Ihrer neuen Funktion nicht benötigt. Dadurch wird das least privilege principle verletzt und gegen gute Praxis verstoßen.

Beobachtung

In Ihrer Umgebung können sämtliche Benutzer und nicht nur Administratoren Sicherheitsgruppen erstellen.

Empfehlung

Wir empfehlen, nur Administratoren das Erstellen von Sicherheitsgruppen zu erlauben. Eine Anleitung zur Konfiguration finden Sie in den Referenzen.

Referenzen

- Anmeldung kann blockiert werden bei Mitgliedschaft in mehr als 2048 Gruppen: https://learn.microsoft.com/de-de/azure/active-directory/conditional-access/concept-conditional-access-users-groups

- Nicht-Administratoren das Recht zum Erstellen von Sicherheitsgruppen entziehen: https://learn.microsoft.com/de-de/azure/active-directory/fundamentals/users-default-permissions#restrict-member-users-default-permissions

Betroffene Ressourcen

Name	Ressourcentyp	Ressourcen ID
Ihre Resource ID	az_tenant	C-Ray