Wie unser Unified Endpoint – und Mobile Device Management „mCloud“ Ihnen hilft, NIS2-Konformität zu erreichen

Die europäische NIS2-Richtlinie bringt neue und strengere Cybersicherheitsvorschriften für viele Branchen. Dies bedeutet für viele Unternehmen, dass sie diese neuen Richtlinien bis Herbst 2024 umsetzen müssen oder sonst hohe Strafen riskieren.

Die seitens der EU geforderte Überarbeitung der Netzwerk- und Informationssysteme bringt einerseits strengere Sicherheitsanforderungen und andererseits erweiterte Meldepflichten mit sich, um Europas kritische Infrastrukturen widerstandsfähiger gegenüber Cyberangriffen zu machen.

Ganz allgemein ist die Reaktion auf Vorfälle und rechtzeitiges Handeln der Schlüssel, um Probleme schnellstmöglich zu beseitigen und die Endgeräte wieder in eine sichere operative Nutzung zu bringen. Besonders IT-Teams müssen jederzeit genau wissen, was auf einem Gerät passiert und im besten Fall (remote) Zugriff auf dieses haben.

In diesem Whitepaper wollen wir Ihnen darstellen, wie unser Unified Endpoint Management (UEM) und Mobile Device Management (MDM) „mCloud“ Ihnen helfen kann, die NIS2-Richtlinie umzusetzen.

Wie unsere mCloud Sie konkret unterstützen kann:

Erkennung und Inventarisierung sämtlicher Endgeräte

- Unsere mCloud ermöglicht Ihnen eine individuelle Organisation der Gerätelandschaft je nach Standort, Betriebssystem, Verwaltungsrechten usw. in der browserbasierenden Konsole.
- Zusätzlich können Sie Tags (ergänzende Kurzbezeichnungen) den Endgeräten hinzufügen umso eine weitere Filter-Möglichkeit zu haben.

barcotec
YOUR DIGITAL ENABLING SPECIALIST.

Sie haben Fragen? Ihr direkter Ansprechpartner Robert Duchac beantwortet Sie gerne:
T +43 1 786 39 40-65 | E duchac@barcotec.at

- Um einen schnellen Überblick über die für Sie wichtigsten Kennzahlen und den Status-Quo Ihrer IT-Landschaft zu haben, können Sie eigene Dashboards erstellen. So haben Sie immer eine gute und transparente Übersicht.
- Ganz generell können Sie mit Hilfe der Konsole jederzeit eine 360-Grad-Ansicht von Geräten, Benutzern und Anwendungen erhalten und entsprechende Reports generieren. So können Sie auch nachverfolgen, ob alle Sicherheitsmaßnahmen umgesetzt wurden und falls nicht, Schwachstellen Management betreiben.

Implementierung einer standardisierten Daten- und Geräteverschlüsselung

- Standardisieren Sie mit Hilfe der mCloud auf allen Geräten die Geräteverschlüsselung, zum Beispiel mit Multi-Faktor-Authentifizierung.
- Mit Hilfe des Kiosk Modus können Sie alle nicht benötigten bzw. potentiell gefährlichen Zugriffe auf dem Gerät unterbinden.
  Ein positiver Nebeneffekt ist, dass die Mitarbeiter eine vereinfachte Arbeitsoberfläche auf ihrem Gerät erhalten und so eine gute Übersicht der von ihnen zu verwendeten Tools haben.
- Weitere Integrationen: SCEP (simple certificate enrollment protocol), SIEM für zentrales Logging via Splunk und Exchange ActiveSync.

Zusammengefasst können Sie somit eine geregelte Zugriffskontrolle erstellen und deren Einhaltung laufend überprüfen.

Homogenes Update- und Patch-Management

- Updates können generell sofort live mit Hilfe eines sogenannten „Jobs“ auf alle Endgeräte ausgespielt werden. Alternativ – je nachdem wie sicherheitskritisch diese Updates sind, können diese natürlich vorbereitet und zu einem späteren Zeitpunkt – z.B. über Nacht – auf die Geräte geschickt werden.
  Dies ist sowohl für Firmware- und Applikationsupdates möglich. Auch Security Patches können so zentral forciert werden.
- Ein weiterer Vorteil ist, dass man mit Hilfe der Reporting-Funktion z.B. täglich eine Information erhält, wer das jeweilige Update schon durchgeführt hat und wer noch nicht.
- Ergänzend kann man die Messaging-Funktion der mCloud nützen, um den Benutzer am Gerät selbst zu informieren, dass ein Update gemacht werden muss – sofern dies nicht zentral gesteuert werden kann oder soll.

Sie haben Fragen? Ihr direkter Ansprechpartner Robert Duchac beantwortet Sie gerne:
T +43 1 786 39 40-65 | E duchac@barcotec.at

„Business Continuity“ mit Hilfe von Backup- und Recoveryprozessen

Im Falle eines Sicherheitsproblems haben Sie mehrere Optionen, die dann vom Team standardisiert abgearbeitet werden können:

- Remote Zugriff auf das Gerät sofern dieses online ist: um einen besseren Überblick neben den Live-Daten zu bekommen, können Sie auf das jeweilige Gerät remote zugreifen – ohne notwendige Aktion des Benutzers.
- Sie können aus der Ferne sämtliche Gerätedaten und -Zugriffe löschen bzw. deaktivieren um weitere Sicherheitsprobleme und eine Ausweitung in das System zu unterbinden.
- Sollte ein Gerätetausch notwendig sein, können Sie mit Hilfe einer hinterlegten Standardkonfiguration ein anderes Gerät neu stagen und so schnellstmöglich für die jeweilige Nutzung zur Verfügung stellen um eine Unterbrechung der operativen Agenden möglichst kurz zu halten. Ist auch eine regelmäßige Abspeicherung sämtlicher Logs hinterlegt, ist auch das Recovery der letzten Arbeitsschritte oder des bisherigen Arbeitstages leichter wiederherstellbar.
- Mit Hilfe der Reporting-Funktion können Sie sich auch automatisiert Status-Updates über Ihre IT-Landschaft zukommen und hier auch proaktiv Schwachstellen-Management betreiben.

Trennung von beruflich und privat bei der Nutzung des Gerätes

- Apps wie WhatsApp oder TikTok auf dem Firmen-Smartphone können gemäß IT-Policy als Sicherheitsrisiko eingestuft und verboten sein. Möchten Sie trotzdem eine umfassende private Nutzung ermöglichen, können Sie auf einem Gerät ein Firmen- als auch ein privates Profil erstellen. Diese sind absolut voneinander getrennt und auch einfache Funktionen wie Kopieren vom beruflichen ins private Profil sind unterbunden.
- Sollte im privaten Profil ein Sicherheitsrisiko auftreten, ist dies von den beruflichen Daten getrennt und erlaubt keine Übergriffe auf diese.

Status-Live-Monitoring und Reporting aller Endgeräte

Eine der größten Vorteile der mCloud ist, dass Sie nicht permanent in der Konsole eingeloggt sein müssen, um einen Geräte-Stauts zu erhalten. Die Reporting-Funktion ist wirklich umfassend und Sie können sowohl live sich Reports generieren als sich diese auch automatisiert (täglich, wöchentlich, monatlich) zusenden lassen.

Reports gibt es zu vielen Gerätedetails und -funktionen:

- sämtliche System Logs inklusive Logs zu App-Installationen oder den zugewiesenen Jobs
- Asset Tracking
- Geräte – und Appnutzung

Sie haben Fragen? Ihr direkter Ansprechpartner Robert Duchac beantwortet Sie gerne:
T +43 1 786 39 40-65 | E duchac@barcotec.at

- Informationen zu allen zugewiesenen Jobs (ob diese alle erfolgreich ausgeführt wurden usw.)
- Gerätedaten wie Batteriestatus, Speicherkapazitäten, Datenverbrauch und Konnektivität
- Compliance: Security Patch Level, Password Policy, Device Encryption, Application Policy uvm.

Sie haben selbstverständlich auch die Möglichkeit, eigene benutzerdefinierte Reports die nur Teile oder eine Mischung der oben genannten Punkte beinhalten, zu erstellen.

Benutzerrechte in der mCloud-Konsole

- Neben verschiedenen Profilen und unterschiedlichen Zugriffsrechten auf den Endgeräten, können Sie auch in der Konsole der mCloud unterschiedliche Benutzerrechte definieren. So haben z.B. nicht alle in Ihrer IT-Abteilung Zugriff auf alle Geräte und Daten. Auch dies können Sie je nach Organisation entsprechend gestalten.
  So können Sie nicht nur die Benutzer der Endgeräte absichern, sondern auch die Benutzer der mCloud-Konsole.
- Eine Vielzahl von Instanzen ist mit Hilfe der sogenannten Mulit-Tenant-Architektur umsetzbar.

Workshops und Trainings

Wie Sie sicherlich erkennen können, ist eine entsprechende Implementierung der mCloud gemäß NIS2-Richtlinien mitunter etwas komplex. Um hier einen guten Plan an der Hand zu haben, erarbeiten wir gerne mit Ihnen gemeinsam in einem 1-Tages-Workshop genau diesen.

Sollten Sie auch Interesse an Schulungen zum Thema Cybersicherheit und Benutzerbewusstsein – speziell für Endgeräte die wir vertreiben – haben, können wir Ihnen diese selbstverständlich ebenfalls anbieten.

Wie funktioniert die mCloud

- Ein sogenannter Agent (Anwendungsdatei) wird auf dem Endgerät installiert und stellt damit die Kommunikation zur Konsole sicher.
- Dann müssen Sie sich nur noch zwischen zwei Lizenzmodellen – „Standard" mit den Basisfunktionen und „Enterprise" mit allen Möglichkeiten der mCloud – entscheiden.
- In weiterer Folge unterstützen wir Sie gerne bei:
  - Migration aus einer anderen Plattform in unsere mCloud
  - Erstkonfiguration und Rollout der Geräte
  - Schulung des IT-Teams für den operativen Einsatz

Sie haben Fragen? Ihr direkter Ansprechpartner Robert Duchac beantwortet Sie gerne:
T +43 1 786 39 40-65 | E duchac@barcotec.at

Fazit und zukünftige Entwicklungen

Die Implementierung eines UEM und MDM verbessert ganz allgemein die Sicherheit Ihrer IT-Landschaft. Zentrales Management und Absicherung aller Endgeräte sind damit einfach für Sie möglich.

Nach NIS kam NIS2 und auch die Technologien selbst entwickeln sich kontinuierlich weiter – damit einhergehend auch die Cyberbedrohungen. Neue Themen wie künstliche Intelligenz werden mittlerweile ebenfalls in UEM-Plattformen integriert, um so möglichst automatisiert und frühzeitig potentiellen Gefahren für die IT-Landschaft erkennen zu können.

Auf Grund dieser Weiterentwicklungen, müssen sich Unternehmen kontinuierlich und agil an neue Richtlinien und Rahmenbedingungen anpassen können – auch deswegen ist die Entscheidung für ein zentrales Management aller Endgeräte aus unserer Sicht unumgänglich.

Kontakt

Zögern Sie nicht, uns zu kontaktieren, um mehr über unsere Dienstleistungen zu erfahren oder individuelle Fragen zu klären. Unsere UEM-Spezialisten beraten Sie gerne persönlich und helfen Ihnen dabei, die passende Lösung für Ihre spezifischen Anforderungen zu finden.

Ihr direkter Ansprechpartner:

Robert Duchac, MA
T +43 1 786 39 40-65
E duchac@barcotec.at