Network-Detektiv

Erstellt für:

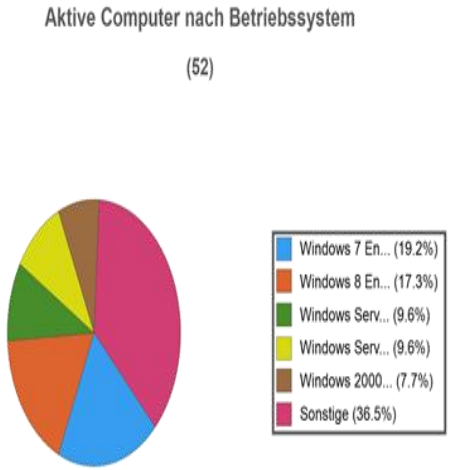
Test

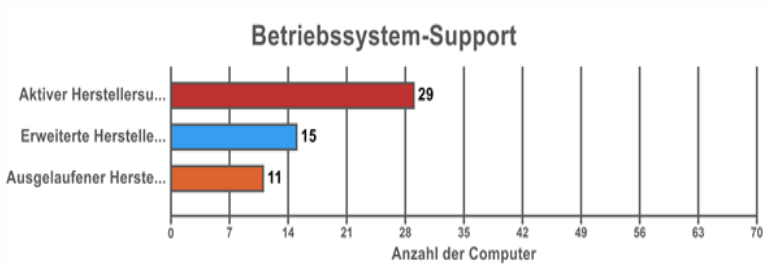
Erstellt von:

Musketier Systemhaus AG

Inhaltsverzeichnis

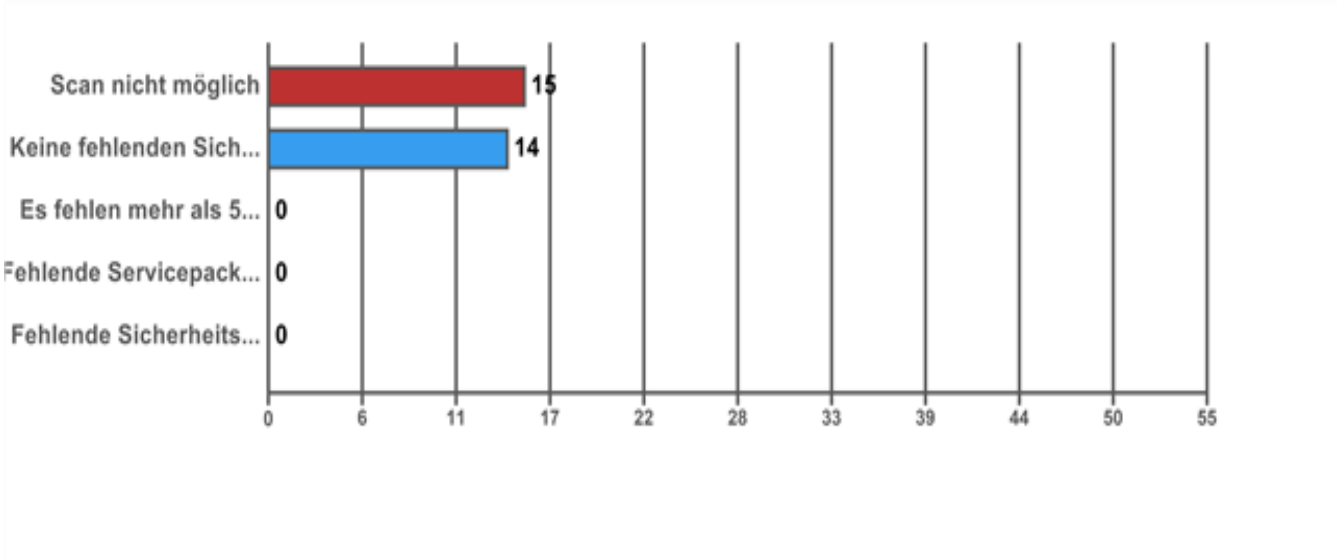
Umgebung - Übersicht





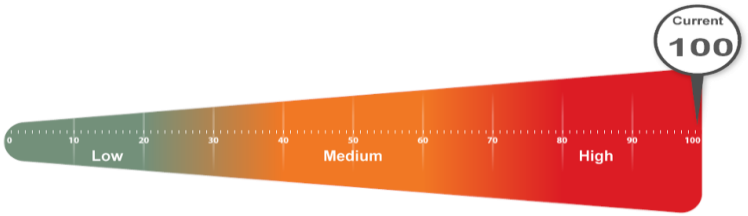
Domäne	
Domänencontroller	4
Anzahl der Organisationseinheiten	13
Benutzer	
# Aktiviert	51
Letzte Anmeldung innerhalb von 30 Tagen	24
Letzte Anmeldung älter als 30 Tage	27
# Deaktiviert	28
Letzte Anmeldung innerhalb von 30 Tagen	0
Letzte Anmeldung älter als 30 Tage	28
Sicherheitsgruppe	
Gruppen mit Benutzern	31
# Alle Gruppen	60
Computer in Domäne	
Alle Computer	153
Letzte Anmeldung innerhalb von 30 Tagen	52
Letzte Anmeldung älter als 30 Tage	101

Umgebung - Patchstatus



Risiko- und Problempunktzahl

Risk Score



Ausgabe Punktzahl

Problemüberprüfung

Mögliche Risiken durch Kennwortstärke (100 pts)
Problem: Bei 2 Benutzerkonten wurde ein potenzial schwach Kennwort befunden. Unzureichend Starke oder schwache Passwörter auf lokale Konten können einem Hacker erlauben, das System zu kompromittieren. Es kann auch auf die Verbreitung von Schadsoftware hinweisen.
Empfehlung: Wir empfehlen, eine ausreichend starke Kennwortrichtlinie zu verwenden um mögliche Risiken zu vermeiden.

Problemüberprüfung

Nicht unterstützte Betriebssysteme/Ausgelaufener Herstellersupport (97 pts)
Problem: Es wurden Computer gefunden, welche ein nicht mehr unterstütztes Betriebssystem nutzen. Nicht unterstützte Betriebssysteme erhalten keine Sicherheitspatches mehr und stellen dadurch ein Sicherheitsrisiko dar.
Empfehlung: Upgraden oder ersetzen Sie die Computer die ein nicht mehr unterstütztes Betriebssystem nutzen.

Problemüberprüfung

Anti-Spyware nicht installiert (94 pts)
Problem: Anti-Spyware-Software wurde auf einigen Computern nicht erkannt. Ohne einen ausreichenden Anti-Virus- und Anti-Spyware-Schutz auf allen Workstations und Servern ist das Risiko bösartiger Software erhöht.
Empfehlung: Um Sicherheitsprobleme zu vermeiden empfehlen wir, einen AntiSpywareschutz auf allen Geräten zu installieren

Problemüberprüfung

Anti-Virus nicht installiert (94 pts)
Problem: Es wurde keine Anti-Virus-Software auf einigen Computern erkannt. Ohne ausreichenden Anti-Virus- und Anti-Spyware-Schutz auf allen Workstations und Servern ist das Risiko erhöht von bösartiger Software infiziert zu werden.
Empfehlung: Um Sicherheitsprobleme zu vermeiden empfehlen wir, einen AntiVirenschutz auf allen Geräten zu installieren

Problemüberprüfung

Anti-Virus nicht eingeschaltet (92 pts)
Problem: Wir waren nicht in der Lage zu bestimmen, ob eine Anti-Viren-Software auf einigen Computern aktiviert ist und ausgeführt wird.
Empfehlung: Feststellen ob AntiVirenschutz aktiviert ist

Problemüberprüfung

Einige Sicherheitspatches fehlen auf einigen Computern (90 pts)
Problem: Sicherheits-Patches fehlen auf eínigen Computern. Sicherheitspatches zu installieren unterstützt bei der Vermeidung von Sicherheitsrisiken. Einige ist definiert als fehlend von 3 oder weniger Patches.
Empfehlung: Aktualisieren Sie die Computer mit fehlenden Sicherheitspatches

Problemüberprüfung

Benutzerkennwörter sind so eingestellt, dass diese niemals ablaufen (80 pts)
Problem: Benutzerkennwörter sind so eingestellt, dass diese niemals ablaufen. Dies kann ein Risiko darstellen, da diese durch die Nutzung durch nicht autorisierte Benutzer leichter verwendet werden können. Diese sind leichter zu hacken/umgehen, als Kennwörter, welche routinemäßig verändert werden.
Empfehlung: Untersuchen Sie alle Konten mit Passwörtern die niemals ablaufen und konfigurieren Sie diese entsprechend.

Problemüberprüfung

Potenzieller Fehler beim Laufwerksspeicher (68 pts)
Problem: 2 Computer wurden mit deutlich wenig freiem Speicherplatz gefunden.
Empfehlung: Freier oder ergänzenden Speicherplatz für die angegebenen Laufwerke hinzufügen.

Problemüberprüfung

Signifikant hohe Anzahl von Domain-Administratoren (35 pts)
Problem: Mehr als 30% der Nutzer sind in der Domain-Administrator-Gruppe und haben uneingeschränkten Zugriff auf Dateien und Systemressourcen. Kompromittierte Domänenadministratorkonten stellen eine höhere Gefahr als normale Benutzer dar.
Empfehlung: Beurteilen Sie die Notwendigkeit, mehr als 30% der Nutzer in der Domänenadministratorgruppe zu haben und den administrativen Zugriff auf das notwendige Minimum zu beschränken.

Problemüberprüfung

Betriebssystem im erweiterten Support (20 pts)
Problem: Es wurden Computer die ein Betriebssystem mit ausgelaufenen Herstellersupport nutzen entdeckt. Ausgelaufene Betriebssysteme erhalten keinen Herstellersupport mehr und werden nicht mehr gepatched.
Empfehlung: Upgrade der Computer die ein Betriebssystem mit ausgelaufenen Herstellersupport nutzen bevor diese End-of-Life sind.

Problemüberprüfung

Inaktive Computer (15 pts)
Problem: Computer haben sich innerhalb der letzten 30 Tage nicht angemeldet
Empfehlung: Prüfen Sie die Liste der inaktiven Computer um festzustellen, ob sie aus dem Active Directory entfernt werden sollten.

Problemüberprüfung

Benutzer hat sich in 30 Tagen nicht angemeldet (13 pts)
Problem: Benutzer, die sich in den letzten 30 Tagen nicht angemeldet haben, könnten Benutzerkonten von ehemaligen Mitarbeiter sein
Empfehlung: Deaktivieren oder entfernen Sie Benutzerkonten, die sich nicht in den letzten 30 Tagen angemeldet haben.

Problemüberprüfung

Ungefüllte Organisationseinheiten (10 pts)
Problem: Leere Organisationseinheiten (OU) im Active Directory gefunden. Diese könnten zu Fehlkonfigurationen führen
Empfehlung: Entfernen oder füllen Sie Organisationseinheiten

Problemüberprüfung

Unsichere offene Ports (10 pts)
Problem: Computer verwenden potenziell unsichere Protokolle.
Empfehlung: Es kann einen legitimen Grund geben, aber die Risiken sollten einzelnen bewerten werden. Bestimmte Protokolle sind von Natur aus unsicher da bspw. typischerweise die Verschlüsselung fehlt. Innerhalb des Netzwerks sollte ihre Verwendung so weit wie möglich minimiert werden, um die Ausbreitung von bösartiger Software zu verhindern. Natürlich kann es Gründe geben diese Dienste und andere Mittel zum Schutz der Systeme erforderlich sind.. Wir empfehlen eine Überprüfung aller Programme für jene die das Netzwerk nutzen um die Notwendigkeit und Sicherheit abzuschätzen.

Nächste Schritte

- Stimme Liste der zu lösenden Probleme zu
- Schätzung der Projektkosten
- Zeitpläne herstellen
- Meilensteine setzen
- Unterschrift erhalten, um Umsetzung durchzuführen