

ΘΕΜΑ 4

4.1. Το αρχείο SAM (Security Account Manager) είναι ένα αρχείο του Λειτουργικού Συστήματος των Windows που περιέχει τα διαπιστευτήρια σύνδεσης, δηλαδή το όνομα χρήστη(username) και τον κωδικό (password) των άλλων χρηστών μεταξύ των οποίων και του διαχειριστή (administrator) στο σύστημα αυτό.

4.2. Ένας κακόβουλος χρήστης θα μπορούσε να αλλάξει τον κωδικό πρόσβασης του διαχειριστή και να χρησιμοποιήσει έναν νέο κωδικό πρόσβασης για να εκτελέσει οποιεσδήποτε εργασίες απαιτούν δικαιώματα διαχειριστή. Μεταξύ αυτών θα μπορούσε να:

- Εγκαταστήσει ή να απεγκαταστήσει προγράμματα στον υπολογιστή.
- Μολύνει με κακόβουλο λογισμικό τον υπολογιστή
- Παρακολουθήσει και να καταγράψει τις κινήσεις των άλλων χρηστών που συνδέονται στον υπολογιστή αυτόν κλπ

4.3. Για την αντιμετώπιση της ευπάθειας αυτής στην έκδοση 20H2 των Windows 10 [1] θα μπορούσαν να προταθούν τα εξής:

- Να γίνει καθαρή εγκατάσταση στους υπολογιστές της εταιρείας, της έκδοσης των Windows 10 ή μεταγενέστερης, και όχι αναβάθμιση από προηγούμενη έκδοση των Windows.
- Να εγκατασταθεί η τελευταία ενημέρωση ασφαλείας με αριθμό CVE-2021-36934 από την Microsoft, στους υπολογιστές αυτούς και επίσης,[2]
- Να διαγραφούν όλα τα σκίωδη αντίγραφα της μονάδας δίσκου του συστήματος των υπολογιστών της εταιρείας, ώστε να μην έχουν πρόσβαση άλλοι χρήστες που δεν είναι εξουσιοδοτημένοι στο αρχείο SAM. [3]

[1] i) <https://techmaniacs.gr/eypatheia-sta-windows-10-epitrepei-se-opoiondipote-na-parei-dikaionata-diacheiristi/> accessed 15/2/22

ii) <https://www.bleepingcomputer.com/news/microsoft/new-windows-10-vulnerability-allows-anyone-to-get-admin-privileges/> accessed 15/2/22

iii) <https://www.windowscentral.com/watch-out-latest-windows-11-and-windows-10-admin-privileges-vulnerability> accessed 15/2/22

[2] <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36934> accessed 15/2/22

[3] <https://support.microsoft.com/el-gr/topic/kb5005357-διαγραφή-αντιγράφων-σκιάς-όγκου-1ceaa637-aaa3-4b58-a48b-baf72a2fa9e7> accessed 15/2/22