Μελέτη περίπτωσης

Όταν το Αεροδρόμιο του Λονδίνου έγινε στόχος μιας καταστροφικής κυβερνοεπίθεσης, οι εκτυπωτές της HP εντόπισαν την απειλή

Επίσημη συνοπτική αναφορά για την παραβίαση δεδομένων

Κλάδος
Αεροπορία

Στόχος
Προσδιορισμός αδύναμων σημείων στις πρακτικές της κυβερνοασφάλειας και αντιμετώπισή τους

Προσέγγιση
Ανάπτυξη ολοκληρωμένου σχεδίου ασφάλειας σε συνεργασία με τους ειδικούς ασφάλειας της HP

Ενέργειες IT
- Εφαρμογή μέτρων ασφάλειας σε τελικά σημεία IoT
- Ενεργοποίηση ενσωματωμένων λειτουργιών ασφάλειας σε εκτυπωτές HP
- Βελτίωση παρακολούθησης της ασφάλειας σε ολόκληρο το δίκτυο

Ενέργειες επιχείρησης
Βελτίωση κυβερνοασφάλειας για την προστασία σημαντικών διεθνών υποδομών και διατήρηση της ασφάλειας των επιβατών

Επισκόπηση

Το Αεροδρόμιο του Λονδίνου* εξυπηρετεί καθημερινά πάνω από 300.000 επιβάτες που ταξιδεύουν σε 94 χώρες σε ολόκληρο τον κόσμο. Στο αεροδρόμιο εργάζονται σχεδόν 50.000 άτομα από 300 εταιρείες, καθιστώντας το ουσιαστικά μια πυκνοκατοικημένη πόλη.

Καθώς το αεροδρόμιο αναπτύσσεται, οι υποδομές του γίνονται ολοένα πιο συνδεδεμένες και αυτοματοποιημένες. Τα εσωτερικά συστήματα, από τη θέρμανση, τον αερισμό και τον κλιματισμό μέχρι το φωτισμό και τους εκτυπωτές ανήκουν πλέον στο δίκτυο του αεροδρομίου. Η εκτύπωση, η σάρωση και η αντιγραφή πραγματοποιούνται από ένα στόλο που αποτελείται από περισσότερους από 60 HP MFP που βρίσκονται σε όλες τις εγκαταστάσεις του αεροδρομίου.

Στις 23 Απριλίου 2018, ο κυβερνοτρομοκράτης που είναι γνωστός ως "The Wolf" χρησιμοποίησε τα συνδεδεμένα συστήματα φωτισμού του αεροδρομίου για να αποκτήσει πρόσβαση και να μεταδώσει το κακόβουλο λογισμικό του στο δίκτυο. Καθώς είναι γνωστός για τις επιθέσεις του στις οποίες χρησιμοποιεί τελικά σημεία με ανεπαρκή προστασία, οι ειδικοί ασφάλειας IT, στο πλαίσιο της έρευνας προκειμένου να απομονώσουν και να σταματήσουν την επίθεση, στράφηκαν αμέσως στα αρχεία καταγραφής απειλών από τους εκτυπωτές HP. Παραδόξως, τα αρχεία καταγραφής περιείχαν στοιχεία που είχε αφήσει ο The Wolf σχετικά με αφορά την προέλευση της εισβολής. Στη συνέχεια, το Αεροδρόμιο του Λονδίνου απευθύνθηκε στην HP για να ενισχύσει περαιτέρω την ασφάλεια των τελικών σημείων του.

Τι συνέβη

Όταν ο The Wolf εντόπισε ένα τρωτό σημείο, πιθανότατα στέλνοντας ηλεκτρονικό phishing email σε χρήστες στο δίκτυο, μπόρεσε να μολύνει το σύστημα φωτισμού IoT με κακόβουλο λογισμικό. Έπειτα μπόρεσε να μεταδώσει το κακόβουλο λογισμικό στο δίκτυο, δημιουργώντας σημεία εισόδου σε άλλες μη επιτηρούμενες συσκευές σε χρήστες.

Καλύπτοντας την παρουσία τους σε συσκευές IoT χωρίς επιτήρηση, τα μέλη της ομάδας του The Wolf μπόρεσαν να παραμείνουν απαρατήρητα από τα συστήματα παρακολούθησης του δικτύου, ενώ ανέπτυξαν πολλά σημεία για την εξαπόλυση μιας μαζικής καταστροφικής επίθεσης.

Η διοίκηση του αεροδρομίου κατέβαλε απεγνωσμένες προσπάθειες για να τερματίσει τη λειτουργία πολλών συστημάτων, ενώ παράλληλα κρίσιμες υποδομές συνέχισαν να λειτουργούν ώστε να μην επηρεαστούν οι πτήσεις και οι επιβάτες.

Αντίδραση στην επίθεση

Ο The Wolf είχε προσληφθεί για να επιτεθεί στο δίκτυο του αεροδρομίου. Το προσωπικό ασφάλειας IT του αεροδρομίου *πίστευε* ότι το δίκτυο του αεροδρομίου ήταν καλά προστατευμένο από τους χάκερ, αλλά δεν είχε αντιληφθεί την επικινδυνότητα των απειλών που κρύβονταν στις συσκευές IoT.

Ευτυχώς, οι εκτυπωτές HP Enterprise του αεροδρομίου διέθεταν το HP Connection Inspector, το οποίο σταμάτησε το κακόβουλο λογισμικό όταν έκανε ύποπτες προσπάθειες να επικοινωνήσει με τους διακομιστές εντολών και ελέγχου των χάκερ.

Οι ενέργειες καταγράφηκαν στα syslog των εκτυπωτών. Όταν το προσωπικό IT κατάλαβε ότι κάτι δεν πήγαινε καλά, έλεγξε τα syslog για λεπτομέρειες σχετικά με την επίθεση. Ωστόσο, ο χρόνος είναι σημαντικός όταν υπάρχει κακόβουλο λογισμικό που εξαπλώνεται στο δίκτυο. Αν το προσωπικό ασφάλειας IT είχε συνδέσει τα syslog εντοπισμού απειλών των εκτυπωτών με το σύστημα παρακολούθησης πληροφοριών και συμβάντων ασφαλείας (SIEM), θα είχε ειδοποιηθεί άμεσα για την εκδήλωση της επίθεσης.

Ισχυρότερη ασφάλεια από ποτέ

Μετά την παραβίαση, το προσωπικό IT εξέτασε τις πρακτικές ασφάλειας με τον πάροχο υπηρεσιών διαχειριζόμενης εκτύπωσης και τους συμβούλους ασφάλειας της HP.

Το Αεροδρόμιο του Λονδίνου, εγκαθιστώντας εκτυπωτές HP Enterprise, είχε ήδη κινηθεί προς τη σωστή κατεύθυνση. Μόνο οι εκτυπωτές και οι συσκευές MFP HP Enterprise προσφέρουν τη δυνατότητα εντοπισμού εισβολών κατά το χρόνο εκτέλεσης και διαθέτουν το HP Connection Inspector για τον εντοπισμό και την εξουδετέρωση κακόβουλου λογισμικού κατά τη διάρκεια της λειτουργίας και την εκτέλεση αναγκαστικής επανεκκίνησης. Κατά την εκκίνηση, το HP Sure Start ελέγχει το BIOS και μπορεί να εκτελέσει αυτόματη αποκατάσταση αν ο κώδικας έχει παραβιαστεί, ενώ η δημιουργία λευκών λιστών (white listing) ελέγχει το υλικολογισμικό.

Ο πάροχος υπηρεσιών διαχειριζόμενης εκτύπωσης ανέπτυξε το HP JetAdvantage Security Manager για να ελέγχονται αυτόματα οι ρυθμίσεις ασφάλειας όποτε γίνεται επανεκκίνηση των εκτυπωτών και να γίνεται επαναφορά τυχόν τροποποιημένων ρυθμίσεων.

Επίσης, το προσωπικό ασφάλειας IT του αεροδρομίου ανέλαβε να συνδέσει τα syslog των εκτυπωτών με το αντίστοιχο εργαλείο SIEM. Σε αντίθεση με τους εκτυπωτές άλλων κατασκευαστών, οι συσκευές HP μπορούν να παρέχουν αρχεία καταγραφής για συγκεκριμένες απειλές σε πολλά εργαλεία SIEM, προκειμένου το προσωπικό IT να μπορεί να λαμβάνει ειδοποιήσεις σε πραγματικό χρόνο για πιθανά συμβάντα ασφάλειας. Έτσι οι εκτυπωτές HP μετατρέπονται στα ανεκτίμητα "μάτια" στο δικτύου τους.

Συμπέρασμα

Λόγω των εκτυπωτών HP Enterprise του αεροδρομίου και των στοιχείων που άφησε ο The Wolf, η ομάδα ασφάλειας μπόρεσε να απομονώσει γρήγορα την επίθεση και να αποφύγει διακοπές λειτουργίας, αρνητική δημοσιότητα, πρόστιμα μη συμμόρφωσης και ζημιά στην εικόνα του αεροδρομίου.

Το αεροδρόμιο βελτίωσε την ασφάλεια στο δίκτυο, εφαρμόζοντας πιο αποτελεσματικές πρακτικές ασφάλειας και αξιοποιώντας πλήρως τις ενσωματωμένες λειτουργίες ασφάλειας των εκτυπωτών HP.

**Το Αεροδρόμιο του Λονδίνου είναι ένας φανταστικός οργανισμός που έγινε στόχος μιας μεγάλης κυβερνοεπίθεσης στην ταινία της HP Studios, "THE WOLF: TRUE ALPHA".*

Για περισσότερες πληροφορίες σχετικά με τις λύσεις της HP:
Ασφάλεια εκτυπώσεων:
hp.com/go/reinventsecurity
Ασφάλεια υπολογιστών:
hp.com/go/ComputerSecurity

Για να δείτε τις ταινίες "The Wolf", επισκεφτείτε τη διεύθυνση: hp.com/thewolf

Εγγραφείτε για ενημερώσεις
hp.com/go/getupdated

Κοινοποιήστε το σε συναδέλφους

4AA7-3560ELE, Αύγουστος 2018