Μελέτη περίπτωσης

Η δοκιμή διείσδυσης δείχνει ότι η παραβίαση κυβερνοασφάλειας της Torvik Industries από τον "The Wolf" θα μπορούσε να είχε αποτραπεί από τους εκτυπωτές HP

Επίσημη συνοπτική αναφορά για την παραβίαση δεδομένων

Κλάδος
Ναυτιλία

Στόχος
Ανάλυση και αντιμετώπιση των τρωτών σημείων του δικτύου

Προσέγγιση
Δοκιμή διείσδυσης για τον εντοπισμό των ευπαθειών που οδήγησαν στην επίθεση

Ευρήματα και προτάσεις
- Εκπαίδευση χρηστών προκειμένου να είναι προσεκτικοί σχετικά με το άνοιγμα ύποπτων email και συνημμένων εκτύπωσης
- Αξιοποίηση εκτυπωτών HP με δυνατότητα εντοπισμού απειλών
- Διαμόρφωση όλων των τελικών σημείων για την ασφάλεια, συμπεριλαμβανομένης της υποδομής που μετακινείται ή βρίσκεται σε προσωρινές τοποθεσίες

Ενέργειες επιχείρησης
Εφαρμογή ισχυρότερων μέτρων ασφάλειας για αποφυγή διακοπών στη ροή εργασιών και βελτίωση της εμπιστοσύνης στην εταιρεία. Βελτίωση των πολιτικών για την παρακολούθηση των τελικών σημείων δικτύου σε προσωρινές τοποθεσίες.

Επισκόπηση

Η Torvik Industries* διακινεί 8 εκατομμύρια κοντέινερ κάθε χρόνο. Για 22.000 κατασκευαστές και χονδρεμπόρους, η Torvik αποτελεί τη ζωτική σύνδεση ανάμεσα στα προϊόντα και τους ανθρώπους σε ολόκληρο τον κόσμο. Στην εταιρεία ανήκουν ναυπηγεία, πλοία, αποθήκες και το σύνολο της τεχνολογίας που υποστηρίζει το εκτεταμένο δίκτυο της Torvik.

Καθώς η εταιρεία αναπτύσσεται, καταβάλλονται μεγάλες προσπάθειες για την προσαρμογή της τεχνολογικής της υποδομής. Παρόλο που το προσωπικό ασφάλειας IT έχει διαμορφώσει τους διακομιστές της εταιρείας, δεν έχει ρυθμιστεί η ασφάλεια ορισμένων εκτυπωτών σε περιφερειακά γραφεία ή σε προσωρινές τοποθεσίες.

Στις 23 Απριλίου 2018, ο κυβερνοτρομοκράτης που είναι γνωστός ως "The Wolf" χρησιμοποίησε έναν μη ασφαλή εκτυπωτή για να σαμποτάρει τις δραστηριότητες της Torvik Industries, από τους υπολογιστές, μέχρι τους γερανούς και τα πλοία με κοντέινερ. Ο σύμβουλος της εταιρείας σε θέματα ασφάλειας χρησιμοποίησε δοκιμή διείσδυσης για να αναλύσει το συμβάν και παρείχε προτάσεις για τη βελτίωση της ασφάλειας και της εκπαίδευσης του προσωπικού.

Τι συνέβη

Καθώς η διοίκηση της Torvik Industries είχε συνήθως την πρωτοβουλία των κινήσεων στα πλέον σημαντικά θέματα, κανείς δεν περίμενε να διεισδύσουν χάκερ στο δίκτυο της εταιρείας σε τέτοιο βαθμό ώστε να σταματήσουν να λειτουργούν οι γερανογέφυρες της και τα πλοία της να αλλάξουν κατεύθυνση στον ανοιχτό ωκεανό.

Το μόνο που έπρεπε να κάνει ο The Wolf ήταν να παραβιάσει έναν εκτυπωτή μεγάλου μεγέθους σε κάποιο εργοτάξιο. Στη συνέχεια, ήταν σε θέση να κινηθεί στο δίκτυο της εταιρείας και να χτυπήσει μεγάλους στόχους στις δραστηριότητές της. Από τη μια στιγμή στην άλλη, αυτή η κορυφαία ναυτιλιακή εταιρεία αντιμετώπισε τεράστια προβλήματα στη λειτουργία της, έστρεψε επάνω της τα βλέμματα της διεθνούς κοινότητας και βρέθηκε αντιμέτωπη με χιλιάδες εξοργισμένους πελάτες.

Πώς συνέβη

Το προσωπικό ασφάλειας IT της εταιρείας νόμιζε ότι η εταιρεία ήταν προστατευμένη. Οι ομάδες που ήταν υπεύθυνες για τα τεχνολογικά θέματα και τη διοικητική μέριμνα παρακολουθούσαν συνεχώς τις διεθνείς δραστηριότητές της για πιθανά προβλήματα ασφάλειας. Είχαν προβλεφθεί ακόμα και διαδικασίες ασφάλειας για τελικά σημεία όπως οι εκτυπωτές. Ωστόσο, παρέβλεψαν κάτι: τη διαμόρφωση ασφάλειας ενός εκτυπωτή μεγάλου μεγέθους που βρισκόταν προσωρινά σε ένα ρυμουλκούμενο όχημα εργοταξίου.

Ο χάκερ δεν είχε καν απευθείας πρόσβαση στον εκτυπωτή. Απλώς έστειλε ένα email με ένα συνημμένο PDF στον υπάλληλο της Torvik που ήταν υπεύθυνος για την εκτύπωση εγγράφων μεγάλων διαστάσεων. Το συγκεκριμένο PDF μετέφερε ένα κρυφό αρχείο Postscript (που μετατράπηκε σε όπλο), το οποίο μπορούσε να ανοίξει και να εκτελεστεί όταν το PDF στάλθηκε στον εκτυπωτή. Όταν ο υπάλληλος έστειλε την εργασία εκτύπωσης, το κακόβουλο λογισμικό ενσωματώθηκε στον εκτυπωτή και μετά εξαπλώθηκε σε ολόκληρο το δίκτυο. Ο χάκερ, μεταφέροντας κρυφά το κακόβουλο λογισμικό σε ένα φαινομενικά "αθώο" συνημμένο email, παρέκαμψε το λογισμικό προστασίας από κακόβουλο λογισμικό στους υπολογιστές της εταιρείας.

Η παραβίαση κατέστη δυνατή επειδή ο εκτυπωτής μεγάλου μεγέθους δεν είχε ισχυρή ενσωματωμένη ασφάλεια, όπως τη δυνατότητα εντοπισμού απειλών. Επίσης, η εταιρεία δεν κατάφερε να παρακολουθεί και να διαχειρίζεται τη διαμόρφωση κάθε μεμονωμένου εκτυπωτή σε όλο το στόλο, όπως τους εκτυπωτές που είχε τοποθετήσει προσωρινά στα περιφερειακά γραφεία.

Αντιμετώπιση της παραβίασης

Η Torvik Industries ανέθεσε σε μια κορυφαία εταιρεία εκτέλεσης δοκιμών διείσδυσης να πραγματοποιήσει μια διεξοδική ανάλυση της κυβερνοασφάλειάς της.

Η ομάδα της δοκιμής διείσδυσης πρότεινε την εγκατάσταση εκτυπωτών HP με ενσωματωμένες λειτουργίες ασφάλειας, όπως είναι η σειρά HP DesignJet με δυνατότητα ασφαλούς εκκίνησης και δημιουργία λευκών λιστών υλικολογισμικού (white listing). Αυτές οι λειτουργίες βοηθούν τον εκτυπωτή να εντοπίζει κώδικα κακόβουλου λογισμικού, να τερματίζει τη λειτουργία του και κατόπιν να ειδοποιεί το τμήμα IT για την ανάγκη επανεγκατάστασης γνήσιου υλικολογισμικού HP.

Επίσης, η ομάδα πρότεινε να χρησιμοποιηθεί η λειτουργία ασφάλειας άμεσης ενεργοποίησης του HP JetAdvantage Security Manager, ενός προγράμματος λογισμικού διαχείρισης ασφάλειας για ολόκληρο το στόλο, προκειμένου να εφαρμόζονται αυτόματα πολιτικές ασφάλειας μόλις προστίθενται συσκευές στο δίκτυο. Το HP Security Manager μπορεί, επίσης, να δημιουργήσει αναφορές συμμόρφωσης που δείχνουν κάθε εκτυπωτή HP, ακόμα και σε απομακρυσμένες ή προσωρινές τοποθεσίες. Αυτό υποδεικνύει ότι τηρούνται οι διαμορφώσεις ασφάλειας του στόλου.

Επιπλέον, ο σύμβουλος για θέματα ασφάλειας πρότεινε την υλοποίηση ενός εκπαιδευτικού προγράμματος που θα βοηθήσει τους υπαλλήλους να αναγνωρίζουν ύποπτα email και να αποφεύγουν την εκτύπωση άγνωστων συνημμένων.

Συμπέρασμα

Η Torvik Industries παραμένει κλονισμένη από τις επιπτώσεις της παραβίασης της κυβερνοασφάλειάς της, καθώς και από την αυξημένη δημοσιότητα που έλαβαν οι αντισυμβατικές απόψεις και οι εγκληματικές ενέργειες του προέδρου της. Ενόσω η εταιρεία επιδιώκει να αναπτύξει μια νέα κατεύθυνση σχετικά με τη διοίκηση, η κατεύθυνση που πρέπει να πάρει ως προς την κυβερνοασφάλεια είναι σαφής: με την επιλογή των εκτυπωτών και των λύσεων της HP, ο επόμενος κυβερνοτρομοκράτης δεν θα είναι καθόλου εύκολο να επιτύχει τους στόχους του.

**Η Torvik Industries είναι μια φανταστική εταιρεία που έγινε στόχος μιας μεγάλης κυβερνοεπίθεσης στην ταινία της HP Studios, "THE WOLF: TRUE ALPHA".*

Για περισσότερες πληροφορίες σχετικά με τις λύσεις της HP:
HP DesignJet: hp.com/go/designjetsecurity
Ασφάλεια εκτυπώσεων: hp.com/go/reinventsecurity
Για να δείτε τις ταινίες "The Wolf", επισκεφτείτε τη διεύθυνση:
hp.com/thewolf

Εγγραφείτε για ενημερώσεις
hp.com/go/getupdated

Κοινοποιήστε το σε συναδέλφους

4AA7-3562ELE, Αύγουστος 2018