ΤΕΧΝΙΚΟ ΕΓΓΡΑΦΟ

ΞΕΚΛΕΙΔΩΤΕΣ ΠΟΡΤΕΣ

ΕΡΕΥΝΑ ΔΕΙΧΝΕΙ ΟΤΙ ΟΙ ΕΚΤΥΠΩΤΕΣ ΜΕΝΟΥΝ ΕΥΑΛΩΤΟΙ ΣΕ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΙΣ

Ενώ οι ομάδες IT εστιάζουν την προσοχή τους σε άλλα τελικά σημεία, η ασφάλεια των εταιρικών εκτυπωτών υστερεί

Οι εκτυπωτές είναι εύκολοι στόχοι: Πάρα πολλοί εκτυπωτές δικτύων δεν έχουν περιορισμούς και δεν ασφαλίζονται αποτελεσματικά.

Οι απειλές ωστόσο είναι πραγματικές και δεν πρέπει να αγνοούνται. Οι εταιρικοί εκτυπωτές έχουν εξελιχθεί σε ισχυρές συσκευές δικτύου και παρουσιάζουν τα ίδια τρωτά σημεία με άλλα τελικά σημεία του δικτύου σας. Καθώς μένουν χωρίς ασφάλεια, αποτελούν σημεία εισόδου με μεγάλες πιθανότητες να δεχτούν κυβερνοεπίθεση. Μπορούν επίσης να επιτρέψουν την πρόσβαση στα οικονομικά και απόρρητα δεδομένα της εταιρείας σας δημιουργώντας έτσι πολύ σοβαρά προβλήματα.

Παρόλα αυτά, μια πρόσφατη έρευνα της Spiceworks κατά την οποία ερωτήθηκαν πάνω από 300 ειδικοί IT εταιρειών, αποκαλύπτει ότι μόνο το 16% όσων ανταποκρίθηκαν πιστεύει ότι οι εκτυπωτές διατρέχουν υψηλό κίνδυνο από απειλές/παραβιάσεις ασφάλειας, ποσοστό σημαντικά μικρότερο συγκριτικά με αυτούς που πιστεύουν το ίδιο για τους επιτραπέζιους/φορητούς υπολογιστές και τις φορητές συσκευές.[1] Η αντίληψη αυτή δείχνει πώς προσεγγίζουν οι ομάδες IT την ασφάλεια των δικτύων. Παρόλο που σχεδόν τρεις στις πέντε επιχειρήσεις εφαρμόζουν πρακτικές ασφάλειας εκτυπωτών, το ποσοστό αυτό είναι πολύ μικρότερο συγκριτικά με τα υπόλοιπα τελικά σημεία, με αποτέλεσμα οι εκτυπωτές να παραμένουν ευάλωτοι, και αυτό τη στιγμή που υπάρχουν εύκολες λύσεις για την προστασία του συγκεκριμένου σημείου εισόδου.

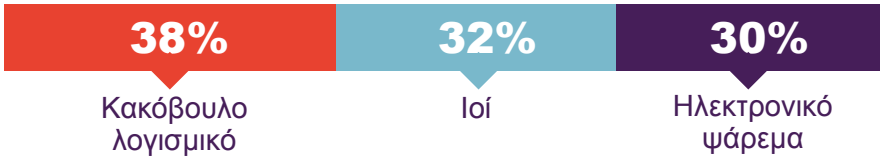
Το παρόν τεχνικό έγγραφο παρουσιάζει δεδομένα ασφάλειας εκτυπωτών βάσει της έρευνας της Spiceworks, τις επιπτώσεις των παραβιάσεων ασφάλειας και κάποια από τα σύγχρονα ενσωματωμένα χαρακτηριστικά ασφάλειας των εκτυπωτών για την προστασία τους από κυβερνοεπιθέσεις.

ΜΟΛΙΣ ΤΟ 16% ΟΣΩΝ ΑΝΤΑΠΟΚΡΙΘΗΚΑΝ ΣΤΗΝ ΕΡΕΥΝΑ ΠΙΣΤΕΥΕΙ ΟΤΙ ΟΙ ΕΚΤΥΠΩΤΕΣ ΔΙΑΤΡΕΧΟΥΝ ΥΨΗΛΟ ΚΙΝΔΥΝΟ ΑΠΟ ΑΠΕΙΛΕΣ/ ΠΑΡΑΒΙΑΣΕΙΣ ΑΣΦΑΛΕΙΑΣ.1

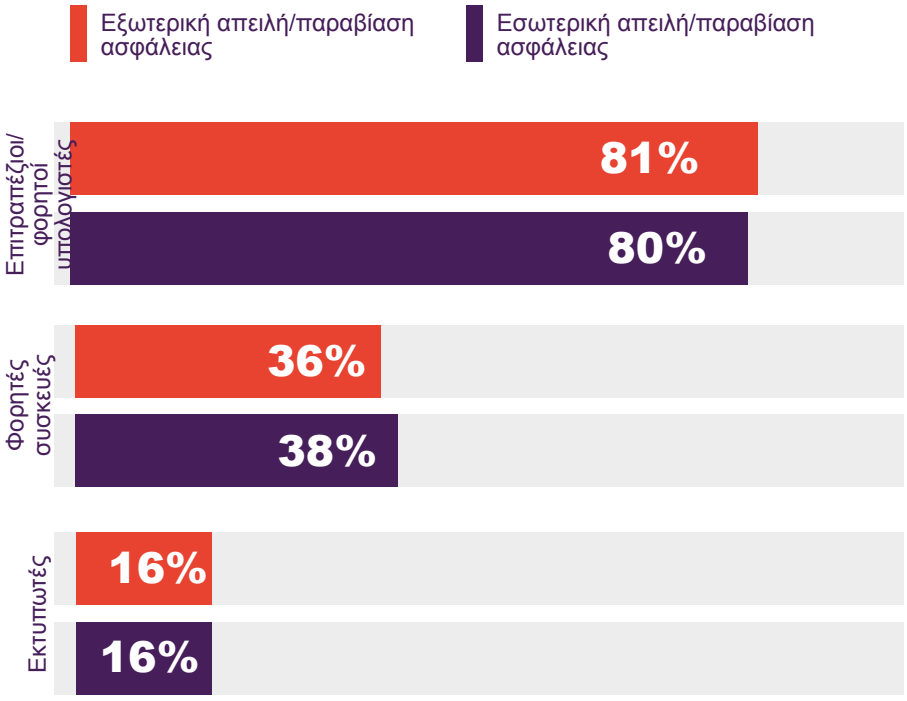
ΠΥΛΗ ΓΙΑ ΕΠΙΘΕΣΕΙΣ

Στην έρευνα της Spiceworks, 74% όσων ανταποκρίθηκαν (καθαρός αριθμός) είπαν ότι η επιχείρησή τους έχει αντιμετωπίσει τουλάχιστον κάποιο είδος εξωτερικής απειλής ή παραβίασης της ασφάλειας IT κατά τη διάρκεια του τελευταίου έτους. Ποσοστό 70% (καθαρός αριθμός) δήλωσε ότι έχουν αντιμετωπίσει κάποια εσωτερική απειλή ή παραβίαση της ασφάλειας IT, με πιο συχνή αιτία κάποιο λάθος οφειλόμενο σε χρήστη, τη χρήση προσωπικών συσκευών για επαγγελματικούς σκοπούς ή επειδή οι εργαζόμενοι χρησιμοποιούσαν οικιακό ή δημόσιο δίκτυο για επαγγελματικούς σκοπούς.[1]

ΣΥΝΗΘΕΙΣ ΕΞΩΤΕΡΙΚΕΣ ΑΠΕΙΛΕΣ/ΠΑΡΑΒΙΑΣΕΙΣ ΑΣΦΑΛΕΙΑΣ IT



Οι πιο συνηθισμένες απειλές εισχώρησαν κυρίως μέσω επιτραπέζιων και φορητών υπολογιστών, ενώ άλλες μέσω φορητών συσκευών και εκτυπωτών.[1] (Το 16% των απειλών που εισχώρησαν μέσω εκτυπωτών είναι σημαντικά υψηλότερο από το 4% που αποκάλυψε παρόμοια έρευνα της Spiceworks το 2014.) Είναι επίσης πιθανόν ο αριθμός των επιθέσεων μέσω εκτυπωτών να μην είναι ο πραγματικός, καθώς οι εκτυπωτές δεν παρακολουθούνται τόσο στενά όσο οι υπολογιστές και οι φορητές συσκευές.



ΠΑΡΑΜΕΛΟΥΜΕ ΤΟΥΣ ΕΚΤΥΠΩΤΕΣ ΜΑΣ

Σε κάθε περίπτωση, η έρευνα της Spiceworks δείχνει ξεκάθαρα ότι η ασφάλεια των εκτυπωτών είναι το τελευταίο που έρχεται στο μυαλό των υπεύθυνων IT.

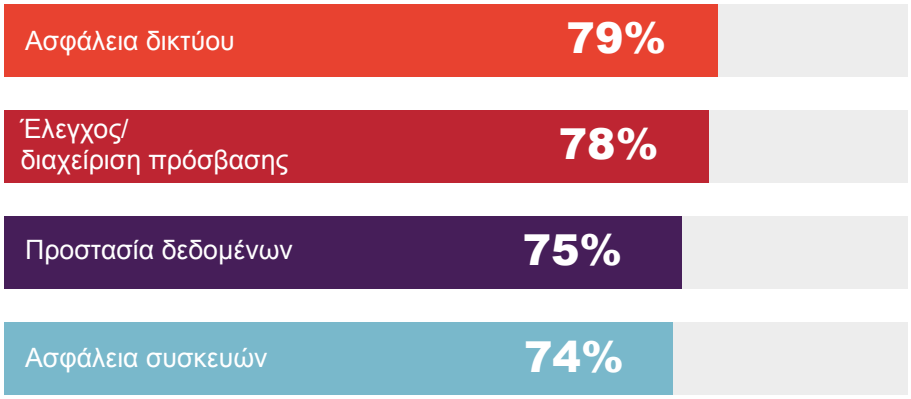
Οι επιχειρήσεις είναι ιδιαίτερα ευαισθητοποιημένες όσον αφορά τη σημασία της ασφάλειας δικτύου, τελικών σημείων και δεδομένων. Στην πραγματικότητα, περισσότεροι από τα 3/4 όσων ανταποκρίθηκαν στην έρευνα χρησιμοποιούν ασφάλεια δικτύου, έλεγχο/διαχείριση πρόσβασης, προστασία δεδομένων, ασφάλεια τελικού σημείου ή συνδυασμό αυτών.[1]

Ωστόσο αυτές οι λύσεις χρησιμοποιούνται πολύ σπανιότερα στους εκτυπωτές. Ενώ 83% των συμμετεχόντων στην έρευνα χρησιμοποιούν ασφάλεια δικτύου στους επιτραπέζιους/φορητούς υπολογιστές και 55% στις φορητές συσκευές, μόλις το 41% τη χρησιμοποιεί στους εκτυπωτές.[1]

Το χάσμα είναι ακόμα μεγαλύτερο όσον αφορά την ασφάλεια τελικού σημείου:

Επιπλέον, ούτε το 1/3 των συμμετεχόντων (28%) δεν χρησιμοποιεί πιστοποιητικά ασφαλείας για τους εκτυπωτές, σε αντίθεση με το 79% και το 54% που τα χρησιμοποιεί για υπολογιστές και φορητές συσκευές αντίστοιχα.[1]

ΣΥΝΗΘΕΙΣ ΠΡΑΚΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ ΤΕΛΙΚΟΥ ΣΗΜΕΙΟΥ



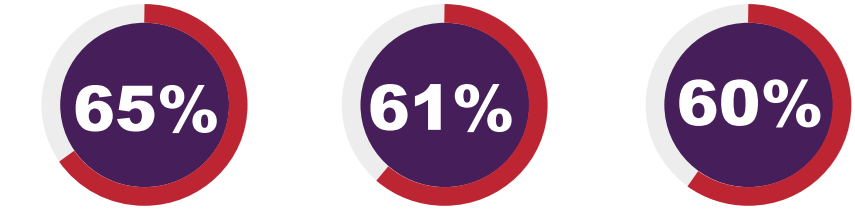
Ανάμεσα στις λύσεις προστασίας που χρησιμοποιούνται στις γενικές συσκευές τελικού σημείου, οι πιο συνηθισμένες για τους εκτυπωτές είναι η ασφάλεια εγγράφων, η ασφάλεια δικτύου και ο έλεγχος πρόσβασης. Ωστόσο λιγότεροι από τους μισούς συμμετέχοντες είπαν ότι η επιχείρησή τους χρησιμοποιεί κάποιες από αυτές τις μεθόδους στους εκτυπωτές της.[1]

Κάποιες εταιρείες εφαρμόζουν πρακτικές ασφάλειας για τους εκτυπωτές, κι εκεί όμως οι μέθοδοι ποικίλλουν σημαντικά. Μόλις πάνω από το 40% των επιχειρήσεων χρησιμοποιεί έλεγχο ταυτότητας χρήστη, και λιγότερο από το 40% χρησιμοποιεί κωδικούς πρόσβασης διαχειριστή για τη διασύνδεση διαμόρφωσης web.[1] Για ισχυρή προστασία, κάθε επιχείρηση θα πρέπει να χρησιμοποιεί ένα συνδυασμό όλων αυτών των μεθόδων, ή και άλλων.

ΣΥΝΗΘΕΙΣ ΠΡΑΚΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ ΕΚΤΥΠΩΤΩΝ

Όσον αφορά τη συμμόρφωση των τελικών σημείων και τις πρακτικές ελέγχου, οι έλεγχοι ασφάλειας στους εκτυπωτές υστερούν συγκριτικά με όλα σχεδόν τα υπόλοιπα τελικά σημεία. Περίπου το 90% των επιχειρήσεων εφαρμόζει κάποια πολιτική ασφάλειας πληροφοριών, αλλά αυτές οι πολιτικές συνήθως δεν καλύπτουν τους εκτυπωτές. Για παράδειγμα, ενώ το 57% των συμμετεχόντων στην έρευνα είπαν ότι χρησιμοποιούν λύσεις προστασίας από κακόβουλο λογισμικό στον υπολογιστή τους, μόλις το 17% χρησιμοποιεί κάποια αντίστοιχη λύση στους εκτυπωτές.[1]

ΣΧΕΔΟΝ 9 ΣΤΟΥΣ 10 ΕΙΔΙΚΟΥΣ IT ΔΗΛΩΝΟΥΝ ΟΤΙ Η ΕΠΙΧΕΙΡΗΣΗ ΤΟΥΣ ΕΦΑΡΜΟΖΕΙ ΚΑΠΟΙΑ ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ ΓΙΑ ΤΟΥΣ ΠΑΡΑΚΑΤΩ ΛΟΓΟΥΣ:



Είναι σαφές ότι οι επιχειρήσεις δεν παίρνουν στα σοβαρά την ασφάλεια των εκτυπωτών. Ωστόσο θα έπρεπε να το κάνουν.

"Πολλοί εκτυπωτές έχουν ακόμα τους εργοστασιακούς κωδικούς πρόσβασης, ή δεν έχουν καθόλου κωδικό πρόσβασης, ή δέκα άτομα χρησιμοποιούν τον ίδιο κωδικό πρόσβασης" είπε ο Michael Howard, υπεύθυνος σύμβουλος ασφάλειας της HP, στην Computerworld τον Ιούνιο. "Ένας εκτυπωτής χωρίς προστασία με κωδικό πρόσβασης είναι χρυσωρυχείο για τους χάκερ. Μία από τις παραβιάσεις που βλέπουμε συχνά είναι οι επιθέσεις man-in-the-middle, όπου κάποιος παίρνει τον έλεγχο του εκτυπωτή και κάνει ανακατεύθυνση [των εισερχόμενων εγγράφων] σε φορητό υπολογιστή πριν την εκτύπωση. Μπορούν να δουν ό,τι εκτυπώνει ο CEO."[2]

ΟΙ ΠΙΘΑΝΕΣ ΕΠΙΠΤΩΣΕΙΣ ΤΩΝ ΕΙΣΒΟΛΩΝ ΣΕ ΕΚΤΥΠΩΤΕΣ

Σύμφωνα με τον Bogdan Botezatu, αναλυτή ηλεκτρονικών απειλών στην Bitdefender, οι εκτυπωτές αποτελούν μια σημαντική πιθανή τρύπα ασφάλειας. "Χρησιμοποιούμε πολλά δεδομένα τηλεμετρίας στα εργαστήρια αξιολόγησης ευπαθειών. Ο δρομολογητής δεν είναι πλέον η χειρότερη συσκευή στο Internet. Τώρα πια είναι ο εκτυπωτής."[3]

Αυτές οι ευπάθειες μπορούν να έχουν μεγάλες επιπτώσεις σε μια επιχείρηση. Με έναν μόνο μη ασφαλή εκτυπωτή, ολόκληρο το δίκτυο συνδεδεμένων συσκευών μπορεί να γίνει ευάλωτο σε επιθέσεις, επιτρέποντας στους χάκερ να κατασκοπεύουν τις συνδεδεμένες συσκευές και να θέσουν σε κίνδυνο την ασφάλεια ολόκληρου του δικτύου.

1. Αύξηση των κλήσεων στο κέντρο υποστήριξης και του χρόνου παροχής υποστήριξης

2. Μείωση παραγωγικότητας/ αποδοτικότητας

3. Αύξηση του χρόνου εκτός λειτουργίας του συστήματος

4. Αύξηση του χρόνου των κλήσεων υποστήριξης

5. Αύξηση εφαρμογής των πολιτικών τελικού χρήστη

Όλοι έχουμε δει τις επιπτώσεις που έχουν οι παραβιάσεις της ασφάλειας. Στην έρευνα της Spiceworks, οι συμμετέχοντες απάντησαν ότι οι πέντε σημαντικότερες επιπτώσεις των παραβιάσεων είναι:[1]

Η παραβίαση ενός εκτυπωτή μπορεί όμως να είναι πολύ σοβαρότερη από αυτό, ιδιαίτερα εάν χρησιμοποιείτε πολυλειτουργικό εκτυπωτή με δυνατότητα ηλεκτρονικής αποθήκευσης των εκτυπωμένων δεδομένων. Οι εργασίες εκτύπωσης που αποθηκεύονται στη μνήμη cache του εκτυπωτή μπορούν να δώσουν στους χάκερ πρόσβαση σε ευαίσθητα προσωπικά ή επαγγελματικά δεδομένα.

Ακόμα πιο ανησυχητικό είναι το γεγονός ότι οι χάκερ μπορούν να αποκτήσουν πρόσβαση στο ευρύτερο περιβάλλον της εταιρείας μέσω μη ασφαλών εκτυπωτών, υποκλέπτοντας στοιχεία όπως οι αριθμοί κοινωνικής ασφάλισης, οικονομικά στοιχεία ή εσωτερικά υπομνήματα και έγγραφα. Αυτές οι κλεμμένες πληροφορίες μπορούν να επηρεάσουν όχι μόνο τους εργαζόμενους αλλά και να χρησιμοποιηθούν από τους ανταγωνιστές ή να προκαλέσουν σοβαρή ζημιά στη φήμη της εταιρείας.

Η ΕΥΚΟΛΗ ΛΥΣΗ: ΕΝΣΩΜΑΤΩΜΕΝΕΣ ΛΕΙΤΟΥΡΓΙΕΣ ΑΣΦΑΛΕΙΑΣ

Είναι σαφές ότι οι εταιρείες πρέπει να ασχοληθούν με την ασφάλεια ακόμα και των εκτυπωτών. Κάποιοι από τους σύγχρονους εκτυπωτές επιχειρηματικής κλάσης διαθέτουν ενσωματωμένα, εύχρηστα χαρακτηριστικά ασφάλειας που αντιμετωπίζουν τις απειλές. Αυτά τα καινοτόμα χαρακτηριστικά είναι τα εξής:

- Αυτόματη ανίχνευση επιθέσεων, προστασία και αποκατάσταση
- Παρακολούθηση για αποτροπή της μη εξουσιοδοτημένης χρήσης
- Απλές επιλογές σύνδεσης όπως το PIN ή οι smartcard
- Συσκευή ανάγνωσης καρτών εγγύτητας που επιτρέπει στους χρήστες να πραγματοποιούν γρήγορο έλεγχο ταυτότητας και να εκτυπώνουν με ασφάλεια χρησιμοποιώντας την ταυτότητά τους
- Ασφαλής κρυπτογραφημένη εκτύπωση για απόρρητα έγγραφα

Αν σκέφτεστε να αγοράσετε καινούριο εκτυπωτή, επιτραπέζιο ή πολυλειτουργικό, ελέγξτε τα ενσωματωμένα χαρακτηριστικά ασφαλείας – και βεβαιωθείτε ότι θα τα ενεργοποιήσετε. Με απλά, ειδικά χαρακτηριστικά σαν αυτά δεν υπάρχει κανένας λόγος να διατηρείτε τρωτά σημεία για την επιχείρησή σας μέσα από τους εκτυπωτές σας. Εξάλλου, στην εποχή του Internet of Things, υπάρχουν πολλά άλλα σημεία πρόσβασης για τα οποία πρέπει να ανησυχείτε – οι εκτυπωτές σας ας μην είναι ένα από αυτά.

ΘΕΛΕΤΕ ΠΙΟ ΑΣΦΑΛΕΙΣ ΕΚΤΥΠΩΤΕΣ;
ΜΑΘΕΤΕ ΠΕΡΙΣΣΟΤΕΡΑ ›

Πηγές:

[1] Έρευνα της Spiceworks σε 309 υπεύθυνους λήψης αποφάσεων σε θέματα IT στη Βόρεια Αμερική, την Ευρώπη, τη Μέση Ανατολή και την Αφρική
(EMEA) και την Ασία Ειρηνικού και την Κίνα (APAC), για λογαριασμό της HP, τον Νοέμβριο 2016.

[2] "Printer Security: Is your company's data really safe?" Computerworld, 1 Ιουνίου 2016.
http://www.computerworld.com/article/3074902/security/printer-security-is-your-companys-data-really-safe.html

[3] "Printers Now the Least-secure Things on the Internet," The Register, 8 Σεπτεμβρίου 2016.
http://www.theregister.co.uk/2016/09/08/the_least_secure_things_on_the_internet/