Microsoft

Σενάρια και λύσεις ασφάλειας στον κυβερνοχώρο με απλούς όρους

Εισαγωγή

Η ασφάλεια των πληροφοριών είναι ένα από τα πιο καυτά θέματα συζήτησης στην πληροφορική τα τελευταία χρόνια. Ο αυξανόμενος αριθμός επιθέσεων από εισβολείς και ιούς, καθώς και οι ιστορίες υψηλής προβολής με δεδομένα που έχουν υποστεί παραβίαση, έχουν προσελκύσει μεγάλη προσοχή στον κόσμο της τεχνολογίας πληροφοριών.

Τα στελέχη συχνά δεν κατανοούν σε βάθος την ασφάλεια των πληροφοριών, τους κινδύνους και τις τρέχουσες απειλές. Συνήθως έχουν μια ιδέα για δύο ή τρεις απειλές που τους απασχολούν γενικά σε προσωπικό επίπεδο και συχνά δεν θέλουν να εμβαθύνουν στις ιδιαιτερότητες του IT. Όταν εγκρίνουν τον προϋπολογισμό τους, είναι σημαντικό γι' αυτούς οι επενδύσεις σε νέο λογισμικό να είναι βέλτιστες από πλευράς κόστους και να έχουν θετικό αντίκτυπο στην επιχείρησή τους.

Αυτό το eBook θα σας βοηθήσει να βρείτε σημεία που μπορείτε να χρησιμοποιήσετε σε συζητήσεις με τους υπεύθυνους λήψης αποφάσεων, χρησιμοποιώντας τη φυσική τους γλώσσα - τη γλώσσα των επιχειρήσεων. Περιγράφει πώς οι λύσεις της Microsoft, όπως το Microsoft 365 και το Microsoft Azure, καθιστούν δυνατή τη μείωση του κινδύνου απειλών για μια επιχείρηση και ενδεχομένως την αποτροπή μιας καταστροφής που προκαλείται από επίθεση από εισβολείς ή από ιό.

Αυτό το eBook είναι μια επικαιροποιημένη έκδοση της έκδοσης του 2018, που ενσωματώνει νέες τεχνολογίες και προκλήσεις.

Πώς να χρησιμοποιήσετε αυτό το eBook

Σε αυτό το eBook θα βρείτε παραδείγματα διαφόρων τύπων επιθέσεων και τρόπους προστασίας από αυτές. Οι περιγραφές παρέχονται χρησιμοποιώντας τόσο τεχνική γλώσσα όσο και γλώσσα κατανοητή από τους υπεύθυνους λήψης αποφάσεων.

Μια προσέγγιση για συζητήσεις σχετικά με την ασφάλεια των πληροφοριών

Μια συζήτηση με τους υπεύθυνους για την ασφάλεια των πληροφοριών έχει τα δικά της μοναδικά χαρακτηριστικά. Οι άνθρωποι συνήθως δεν δίνουν σημασία στην ασφάλεια εφόσον "όλα είναι εντάξει". Οι εταιρείες που έχουν βιώσει σημαντική απώλεια δεδομένων λόγω ιών κρυπτογράφησης δίνουν σημαντικά μεγαλύτερη προσοχή στην ασφάλεια από εκείνες που δεν έχουν αντιμετωπίσει ακόμη προβλήματα. Από την άλλη πλευρά, 100% ασφάλεια δεν υφίσταται. Όσο ένα σύστημα λειτουργεί, εκτίθεται σε κινδύνους. Καθήκον μας είναι να καταδείξουμε την ύπαρξη κινδύνων και να τους μειώσουμε σε αποδεκτό επίπεδο. Επειδή η μείωση του κινδύνου βασίζεται στην αγορά προϊόντων λογισμικού, είναι σημαντικό να βρεθεί η ισορροπία όπου είναι πιο επικερδές να πληρώνεις για την ασφάλεια από το να πληρώνεις για την απουσία της.

Οι κύριες προκλήσεις που αντιμετωπίζουν οι επιχειρήσεις στον τομέα της ασφάλειας των πληροφοριών

01 **Οι άνθρωποι είναι ο πιο αδύναμος κρίκος.**
Συχνά δεν γνωρίζουν την αξία των πληροφοριών με τις οποίες εργάζονται και είναι αρκετά απρόσεκτοι με την προστασία τους.

Η κατάσταση έχει επιδεινωθεί με τη μετάβαση των εργαζομένων στην εξ αποστάσεως εργασία για διάφορους λόγους: οι οικιακές συσκευές είναι λιγότερο ασφαλείς από τις εταιρικές, οι χρήστες των συσκευών έχουν απεριόριστη πρόσβαση και δεν χρειάζεται να παραβιαστεί ο κωδικός πρόσβασης Wi-Fi, επειδή κάποιος μπορεί απλώς να τον ζητήσει.

02 **Διαθεσιμότητα εργαλείων.**
Σήμερα, είναι σχετικά εύκολο να γίνει κάποιος εισβολέας. Έχουν δημιουργηθεί χιλιάδες προσβάσιμα εργαλεία τα οποία μπορεί να κατεβάσει δωρεάν οποιοσδήποτε αρχάριος. Αυτός είναι ο λόγος για τον οποίο ο αριθμός των λεγόμενων "εισβολέων" είναι αρκετά μεγάλος αυτές τις μέρες. Τέτοιοι "εισβολείς" είναι απίθανο να εισβάλουν σε μια καλά προστατευμένη υποδομή, ωστόσο εταιρείες που δεν δίνουν προσοχή στην ασφάλεια των πληροφοριών εμπίπτουν στην ομάδα κινδύνου.
Οι αρχάριοι εισβολείς έχουν γίνει πιο επιτυχημένοι με τη μετάβαση των εργαζομένων στην εξ αποστάσεως εργασία.

03 **Η εταιρεία μας είναι τόσο μικρή - ποιος θα ενδιαφερόταν για εμάς;**
Αυτή είναι μια ευρέως διαδεδομένη άποψη μεταξύ πολλών εταιρειών. Ακόμη και οι μικρές εταιρείες μπορεί να είναι ο στόχος μιας σκόπιμης επίθεσης, αλλά ένα ακόμη μεγαλύτερο πρόβλημα είναι ότι οι επιτιθέμενοι δεν επιλέγουν τους στόχους τους. Οι επιθέσεις είναι αυτοματοποιημένες και στοχεύουν οτιδήποτε μπορεί να δεχθεί επίθεση. Αφότου μια επίθεση είναι επιτυχής, ο επιτιθέμενος θα δει πώς μπορεί να χρησιμοποιήσει τις πληροφορίες που απέκτησε. Στην πράξη, υπήρξαν γνωστές περιπτώσεις όπου εισβολείς προσπάθησαν να παραβιάσουν διακομιστές κυβερνητικών υπηρεσιών από έναν παραβιασμένο εταιρικό διακομιστή. Οι εταιρείες ανακάλυψαν ότι είχαν υποστεί εισβολή όταν οι υπηρεσίες ασφαλείας πήγαν να τους μιλήσουν και να κατασχέσουν τον εξοπλισμό τους.

04 **Ξεπερασμένες τεχνολογίες.**
Το πρόβλημα με την ξεπερασμένη τεχνολογία είναι ότι οι τεχνολογίες αυτές σχεδιάστηκαν για να προστατεύουν από απειλές που ήταν επίκαιρες όταν δημιουργήθηκε το εν λόγω λογισμικό. Όσο περισσότερο το λογισμικό παραμένει στην αρχική του κατάσταση, χωρίς ενημερώσεις, τόσο περισσότερες επιθέσεις από τις οποίες δεν προσφέρει προστασία εμφανίζονται. Δεν μπορούν να αποτραπούν όλες οι επιθέσεις με την "ενημέρωση κώδικα" σε ξεπερασμένη τεχνολογία.

05 **Έλλειψη ειδικών στην ασφάλεια πληροφοριών και ανεπαρκής προσοχή στην ασφάλεια πληροφοριών από τους ειδικούς πληροφορικής.**
Ορισμένες εταιρείες δεν διαθέτουν καν ειδικούς σε θέματα ασφάλειας πληροφοριών. Οι λειτουργίες ασφάλειας των πληροφοριών τους εκτελούνται από έναν ειδικό πληροφορικής. Το πρόβλημα είναι ότι η δουλειά τους είναι να παρέχουν μια λειτουργική υπηρεσία πληροφορικής και η ασφάλεια μπορεί να δυσχεράνει την παροχή αυτής της υπηρεσίας. Για παράδειγμα, ένα προσεκτικά ρυθμισμένο τείχος προστασίας μπορεί να εμποδίσει την εκτέλεση νόμιμων εφαρμογών. Ο ειδικός πληροφορικής πρέπει να επιλέξει: να παρακολουθεί τις θύρες που χρησιμοποιούνται από την εφαρμογή ή να απενεργοποιήσει το τείχος προστασίας. Η δεύτερη επιλογή είναι πιο εύκολη, οπότε κάποιοι θα την επιλέξουν.

Σενάρια και λύσεις

Απειλή

Ένας κωδικός πρόσβασης ηλεκτρονικού ταχυδρομείου μπορεί να βρεθεί, να ζητηθεί ή να ληφθεί από τη μνήμη του προγράμματος περιήγησης

Λύση

Microsoft 365: Έλεγχος ταυτότητας πολλών παραγόντων (multifactor authentication)

Ρύθμιση παραμέτρων ελέγχου ταυτότητας δύο παραγόντων για το Microsoft 365

Με όρους πληροφορικής

Πιθανώς γνωρίζετε ότι πολλοί χρήστες δεν αντιλαμβάνονται τους κωδικούς πρόσβασης ως έναν τρόπο προστασίας από μη εξουσιοδοτημένη πρόσβαση, αλλά ως "σχέδια των διαχειριστών". Αντιμετωπίζουν τους κωδικούς πρόσβασης πολύ επιπόλαια, ενώ απαιτούν από την υπηρεσία πληροφορικής τους να λογοδοτεί για την ασφάλεια των πληροφοριών.

Ο έλεγχος ταυτότητας πολλών παραγόντων (multifactor authentication) απαιτεί από τους χρήστες όχι μόνο να γνωρίζουν τον κωδικό πρόσβασής τους, αλλά και να είναι υπεύθυνοι για τις προσωπικές τους συσκευές. Είναι εύκολο να τον ρυθμίσετε για διαδικτυακές υπηρεσίες και επιλύει μια σειρά από προβλήματα ασφαλείας.

Μπορεί να περιλαμβάνει τηλεφωνική κλήση, SMS, επιβεβαίωση σε μια εφαρμογή για κινητές συσκευές ή την εισαγωγή ψηφίων από μια εφαρμογή για κινητές συσκευές, ενώ υπάρχουν ευέλικτες ρυθμίσεις αποκλεισμού. Για παράδειγμα, μπορεί να μην απαιτείται ο δεύτερος παράγοντας όταν ένας χρήστης εργάζεται από μια διεύθυνση IP της εταιρείας, αλλά να απαιτείται όταν εργάζεται από το σπίτι του.

Ακόμη και αν υπάρξει διαρροή ασφαλείας, η ευθύνη θα βαρύνει εξ ολοκλήρου τους χρήστες, επειδή δεν πρόσεχαν τους κωδικούς πρόσβασης και τις προσωπικές τους συσκευές.

Εξασφαλίστε την υποστήριξη της διοίκησης. Διαφορετικά, ο έλεγχος ταυτότητας πολλών παραγόντων (multifactor authentication) θα εκληφθεί ως το επόμενο "σχέδιο των διαχειριστών".

Με επιχειρηματικούς όρους

Ένας κωδικός πρόσβασης από μόνος του δεν είναι πλέον αρκετός. Οι άνθρωποι επισυνάπτουν αυτοκόλλητες σημειώσεις με κωδικούς πρόσβασης, τους γράφουν σε αρχεία, τους λένε ο ένας στον άλλον και τους αποθηκεύουν σε προγράμματα περιήγησης. Οι κωδικοί πρόσβασης είναι συχνά πολύ απλοί, ώστε να είναι εύκολο για τους χρήστες να τους θυμούνται. Επίσης, οι χρήστες χρησιμοποιούν τα ίδια ονόματα χρήστη και κωδικούς πρόσβασης για να εγγραφούν σε διάφορες τοποθεσίες και φόρουμ με αμφισβητήσιμες ρυθμίσεις ασφαλείας.

Όταν συνδέεστε στην ηλεκτρονική σας τράπεζα, εκτός από τον κωδικό πρόσβασής σας, πρέπει να εισάγετε έναν κωδικό από ένα SMS. Γιατί να προστατεύονται λιγότερο τα επιχειρηματικά σας έγγραφα;

Εξηγήστε στους υπαλλήλους σας ότι τα επιπλέον 15 δευτερόλεπτα που απαιτούνται για την εισαγωγή ενός μηνύματος κειμένου είναι ένα λογικό τίμημα για την προστασία της πρόσβασης σε σημαντικές πληροφορίες.

Απειλή

Ξεχασμένος κωδικός πρόσβασης

Λύση

Microsoft 365: Επαναφορά κωδικών πρόσβασης από τους χρήστες

Με όρους πληροφορικής

Όλα τα πρωινά στα τμήματα πληροφορικής ξεκινούν με τον ίδιο τρόπο: οι χρήστες καλούν για να ζητήσουν βοήθεια με την επαναφορά των ξεχασμένων κωδικών πρόσβασης. Επιτρέποντας στους χρήστες να επαναφέρουν τους δικούς τους κωδικούς πρόσβασης με εναλλακτικές μεθόδους σύνδεσης, μειώνεται σημαντικά ο αριθμός των κλήσεών τους.

Εσείς οι ίδιοι καθορίζετε τις μεθόδους που θα είναι διαθέσιμες στους χρήστες για την επαναφορά των κωδικών πρόσβασής τους. Για παράδειγμα: SMS, μια εφαρμογή για κινητές συσκευές, ερωτήσεις ασφαλείας ή μια προσωπική διεύθυνση ηλεκτρονικού ταχυδρομείου. Μπορείτε να απαιτείτε μία επιλογή ή συνδυασμό δύο επιλογών.

Αυτή η λειτουργία μπορεί να ενσωματωθεί στην τοπική υπηρεσία καταλόγου Active Directory. Ένας κωδικός πρόσβασης του οποίου η επαναφορά έγινε στο cloud θα συγχρονιστεί με την τοπική υπηρεσία καταλόγου Active Directory εντός ενός λεπτού.

Όπως κάθε νέα λύση, οι χρήστες θα χρειαστούν χρόνο για να προσαρμοστούν σε αυτήν. Το καθήκον σας θα είναι όχι μόνο να υλοποιήσετε τη λειτουργία επαναφοράς κωδικού πρόσβασης, αλλά και να ενημερώσετε τους χρήστες σχετικά με αυτήν με κατάλληλες οδηγίες.

Με επιχειρηματικούς όρους

Έχετε ξεχάσει ποτέ τον κωδικό πρόσβασης για το ηλεκτρονικό ταχυδρομείο ή τον υπολογιστή της εταιρείας σας; Συμβαίνει στους υπαλλήλους σας εξίσου συχνά.

Εκτός από την ταλαιπωρία και τον χαμένο χρόνο που δαπανάται σε κλήσεις προς το τμήμα πληροφορικής, μπορεί επίσης να δημιουργήσει πρόσθετους κινδύνους για την ασφάλεια. Κατά την εξ αποστάσεως εργασία, είναι δύσκολο να επαληθεύσετε ότι ο καλών είναι αυτός που ισχυρίζεται ότι είναι.

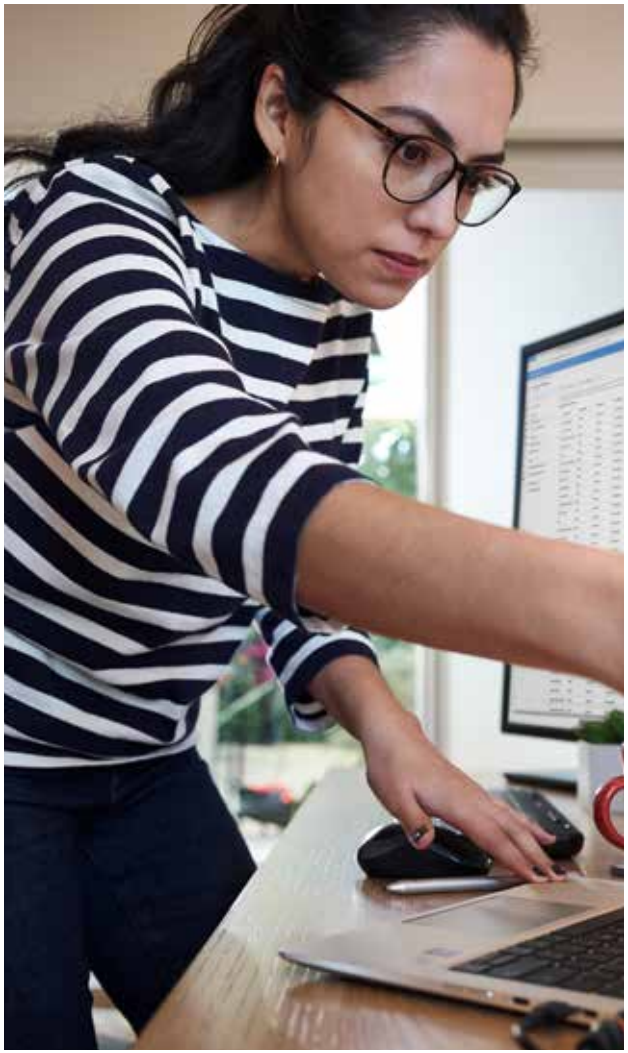
Μια απλή και αποτελεσματική λύση θα ήταν να επιτρέπεται στον χρήστη να επαναφέρει τον κωδικό πρόσβασής του μέσω SMS, ερωτήσεων ασφαλείας ή ενός ειδικού κωδικού σε μια εφαρμογή για κινητές συσκευές.

Απειλή

Χρήση αδύναμων κωδικών πρόσβασης

Λύση

Microsoft 365: Έλεγχος ταυτότητας χωρίς κωδικό πρόσβασης



Με όρους πληροφορικής

Το Azure AD, το οποίο εκτελεί τον έλεγχο ταυτότητας στο Microsoft 365, διαθέτει μια επιλογή για την αποφυγή ορισμού κωδικών πρόσβασης. Το σύνολο των επιλογών είναι αρκετά εκτεταμένο:

01 Μια κινητή συσκευή καταχωρείται ως συσκευή χρήστη. Κατά τη διάρκεια μιας προσπάθειας ελέγχου ταυτότητας, εμφανίζεται ένας αριθμός στην οθόνη και η εφαρμογή Microsoft Authenticator εμφανίζει διάφορους αριθμούς από τους οποίους μπορεί να επιλέξει ο χρήστης. Ο χρήστης επιλέγει τον σωστό αριθμό και, κυρίως, επιβεβαιώνει την ταυτότητά του στην κινητή συσκευή με ένα δακτυλικό αποτύπωμα.

02 Κλειδί υλικού. Χρησιμοποιούνται ένα συμβατό κλειδί υλικού και πρόσθετα δεδομένα.

03 Βιομετρικά δεδομένα.

04 Χαρακτηριστικά που δεν υποστηρίζονται στο Azure AD. Με τη διαμόρφωση μιας ομοσπονδίας μεταξύ της τοπικής υπηρεσίας καταλόγου AD και του Azure AD, οι επιλογές ελέγχου ταυτότητας μπορούν να επεκταθούν. Για παράδειγμα, μπορούν να χρησιμοποιηθούν έξυπνες κάρτες για έλεγχο ταυτότητας.

Κάθε επιλογή έχει τις δικές της δυνατότητες, απαιτήσεις και πεδία εφαρμογής. Δείτε τις δυνατότητες στη διεύθυνση https://docs.microsoft.com/el-gr/azure/active-directory/authentication/concept-authentication-passwordless

Οι περισσότερες εταιρείες βρίσκονται ακόμη στα αρχικά στάδια της μετάβασης στον έλεγχο ταυτότητας χωρίς κωδικό πρόσβασης, οπότε δεν είναι ακόμα μια οικεία διαδικασία. Η διαδικασία μετάβασης στον έλεγχο ταυτότητας χωρίς κωδικό πρόσβασης πρέπει να είναι σταδιακή και η προστασία με κωδικό πρόσβασης δεν πρέπει να παραμελείται μέχρι να ολοκληρωθεί.

Με επιχειρηματικούς όρους

Φανταστείτε μία από τις ακόλουθες περιπτώσεις:

01 Ένας ή περισσότεροι από τους υπαλλήλους σας έλαβαν ένα μήνυμα ηλεκτρονικού ταχυδρομείου σε μορφή Word ή PDF από έναν από τους συνεργάτες σας. Κατά το άνοιγμα του εγγράφου, βλέπουν μια μεγάλη ποσότητα κρυπτογραφημένου κειμένου και το μήνυμα "Αυτό το έγγραφο περιέχει προσωπικά δεδομένα. Για λόγους νομικής συμμόρφωσης, το έγγραφο έχει κρυπτογραφηθεί. Εισαγάγετε τη διεύθυνση ηλεκτρονικού ταχυδρομείου σας και τον κωδικό πρόσβασής σας για να το αποκρυπτογραφήσετε."

02 Ένας υπάλληλος του λογιστηρίου λαμβάνει ένα μήνυμα από τις φορολογικές αρχές σχετικά με μια οφειλή και μια πρόσκληση να χρησιμοποιήσει έναν σύνδεσμο για να δει λεπτομέρειες σχετικά με την οφειλή. Όταν κάνει κλικ στον σύνδεσμο, του ζητείται να εισαγάγει τη διεύθυνση ηλεκτρονικού ταχυδρομείου και τον κωδικό πρόσβασής του.

Αυτά είναι δύο παραδείγματα ηλεκτρονικού "ψαρέματος", σκοπός του οποίου είναι η απόκτηση των κωδικών πρόσβασης των εργαζομένων.

Ο κωδικός πρόσβασης είναι ένας από τους πιο αδύναμους κρίκους και θα πρέπει κάποτε να εξαλειφθεί.

Πώς αποκτάτε πρόσβαση στην κινητή σας συσκευή; Πιθανότατα με δακτυλικό αποτύπωμα. Αυτός είναι ένας τύπος ελέγχου ταυτότητας χωρίς κωδικό πρόσβασης που έχει ήδη ενσωματωθεί σε μεγάλο βαθμό στη ζωή μας με τις κινητές συσκευές μας. Είναι πιο ασφαλής επειδή είναι πολύ δύσκολο να χρησιμοποιηθεί χωρίς τη φυσική σας παρουσία και είναι πιο βολικός επειδή δεν χρειάζεται να αλλάζετε τον κωδικό πρόσβασής σας κάθε ορισμένο αριθμό ημερών.

Τώρα, αυτή η αρχή εφαρμόζεται σε επιχειρηματικά συστήματα για να παρέχει την ασφάλεια και την ευκολία που πιθανώς έχετε ήδη συνηθίσει όταν εργάζεστε με την κινητή σας συσκευή. Εάν ένας εργαζόμενος δει μια προτροπή για την εισαγωγή κωδικού πρόσβασης, θα εγείρει υποψίες επειδή η εταιρεία του δεν χρησιμοποιεί κωδικούς πρόσβασης.

Απειλή

Χρήση παραβιασμένων κωδικών πρόσβασης από τους χρήστες

Λύση

Microsoft 365: Προστασία με κωδικό πρόσβασης

Με όρους πληροφορικής

Αποκλείστε τις λέξεις που δεν πρέπει να χρησιμοποιούνται ως κωδικός πρόσβασης, όπως η επωνυμία της εταιρείας. Δεν θα αποκλειστεί μόνο η λέξη, αλλά και τα παράγωγά της.

Για περισσότερες πληροφορίες, ανατρέξτε στη διεύθυνση https://docs.microsoft.com/el-gr/azure/active-directory/authentication/concept-password-ban-bad

Αυτή η δυνατότητα λειτουργεί για λογαριασμούς cloud και ενσωματώνεται επίσης στην τοπική υπηρεσία καταλόγου Active Directory.

Με επιχειρηματικούς όρους

Ποιες λέξεις θα δοκιμάσει ένας εισβολέας κατά την προσπάθειά του να μαντέψει έναν κωδικό πρόσβασης; Πιθανώς κάτι που σχετίζεται με το όνομα ή το επώνυμό σας και την επωνυμία της εταιρείας σας.

Οι υπάλληλοί σας δεν θα μπορούν να χρησιμοποιούν ως κωδικό πρόσβασης λέξεις που είναι εύκολο να μαντέψει κανείς και το τμήμα πληροφορικής σας θα δημιουργήσει έναν κατάλογο αυτών των λέξεων.

Απειλή

Μη εξουσιοδοτημένη πρόσβαση από μη αξιόπιστες τοποθεσίες

Λύση

Microsoft 365: Περιορισμοί πρόσβασης με χρήση γεωτοποθεσίας

Με όρους πληροφορικής

Το Azure AD παρέχει τη δυνατότητα Πρόσβασης υπό όρους, η οποία είναι ένα από τα βασικά του χαρακτηριστικά. Μπορεί να χρησιμοποιηθεί για την ενεργοποίηση του MFA, για την απαίτηση από τους χρήστες να αλλάζουν τους κωδικούς πρόσβασής τους, για την αποτροπή σύνδεσής τους από τις προσωπικές τους συσκευές κ.λπ.

Ένα από τα χαρακτηριστικά που πρέπει να λαμβάνονται υπόψη πάνω απ' όλα είναι ο περιορισμός των συνδέσεων από μη αξιόπιστες γεωγραφικές τοποθεσίες.

Δημιουργείτε λίστες τοποθεσιών με βάση δημόσιες διευθύνσεις IP ή τις αντίστοιχες γεωγραφικές τοποθεσίες τους. Οι λίστες μπορεί να είναι "επιτρεπόμενες" ή "αποκλεισμού".

Με επιχειρηματικούς όρους

Πιθανότατα έχετε ακούσει ότι οι εισβολείς κρύβουν τις τοποθεσίες τους για να παραμένουν ανώνυμοι. Ακόμη και αν ο εισβολέας είναι γείτονάς σας, η χώρα από την οποία προσπαθεί να συνδεθεί μαζί σας θα είναι διαφορετική.

Υπάρχουν περισσότερες από 200 χώρες στον κόσμο. Γιατί να επιτρέψετε την πρόσβαση στα δεδομένα σας από όλες τις υπάρχουσες χώρες;

Μια απλή λύση είναι να επιτρέπετε τη σύνδεση μόνο από ορισμένες χώρες, ο κατάλογος των οποίων θα καταρτιστεί από το τμήμα πληροφορικής σας.

Απειλή

Συμμόρφωση με τις κανονιστικές απαιτήσεις

Λύση

Microsoft 365: Πολιτικές αποθήκευσης

Με όρους πληροφορικής

Κάθε χρόνο, οι κυβερνήσεις αυστηροποιούν τις απαιτήσεις για τους χώρους αποθήκευσης δεδομένων. Αναδύονται εξωεδαφικές απαιτήσεις όπως ο ΓΚΠΔ. Η συμμόρφωση με αυτές ρυθμίζεται με ένα σύνολο τόσο "γραφειοκρατικών" όσο και τεχνικών μέτρων.

Αυτή η συμμόρφωση είναι μια πολύπλοκη διαδικασία που υπερβαίνει τόσο το πεδίο εφαρμογής αυτού του οδηγού όσο και την ικανότητα ενός τμήματος πληροφορικής.

Ωστόσο, μία σημαντική απαίτηση είναι σχετική για τις περισσότερες εταιρείες: η προστασία των πληροφοριών από τυχαία/εσκεμμένη διαγραφή.

Οι πολιτικές αποθήκευσης καθιστούν δυνατά τα εξής:

01 Εγγύηση αποθήκευσης εγγράφων για συγκεκριμένο χρονικό διάστημα.

02 Αυτόματη διαγραφή εγγράφων μετά από ένα καθορισμένο χρονικό διάστημα.

03 Αποστολή ενός μηνύματος, μετά τη λήξη της περιόδου, στο άτομο που είναι υπεύθυνο να αποφασίσει αν το έγγραφο θα διαγραφεί ή θα αποθηκευτεί για μεγαλύτερο χρονικό διάστημα.

Με επιχειρηματικούς όρους

Σημαντικά έγγραφα μπορούν να διαγραφούν ή να τροποποιηθούν.

Αυτό θα μπορούσε να οδηγήσει όχι μόνο στην απώλεια σημαντικών πληροφοριών, αλλά και σε πρόστιμα από τις ρυθμιστικές αρχές.

Το τμήμα πληροφορικής αποθηκεύει αντίγραφα εγγράφων για γρήγορη ανάκτηση, αλλά τι γίνεται αν το έγγραφο δημιουργήθηκε πριν από τρία χρόνια; Σύμφωνα με τον νόμο, ορισμένα έγγραφα πρέπει να αποθηκεύονται για πολλά χρόνια.

Οι πολιτικές αποθήκευσης θα προστατεύουν σημαντικά έγγραφα, μηνύματα ηλεκτρονικού ταχυδρομείου, ακόμη και μηνύματα συνομιλίας από τυχαία ή σκόπιμη διαγραφή κατά τη διάρκεια της επιλεγμένης περιόδου.

Απειλή

Κακόβουλα συνημμένα ηλεκτρονικού ταχυδρομείου

Λύση

Microsoft 365: Ασφαλή συνημμένα

Προφίλ και ρύθμιση παραμέτρων των ασφαλών συνημμένων Office 365 ATP

Με όρους πληροφορικής

Κάθε συνημμένο εκτελείται στο δικό του sandbox υλικού στο κέντρο δεδομένων της Microsoft. Μέχρι το σύστημα να επαληθεύσει ότι το συνημμένο αρχείο είναι ασφαλές, δεν παραδίδεται στον χρήστη. Πραγματοποιείται ανάλυση της συμπεριφοράς του συνημμένου.

Ο διαχειριστής μπορεί να λάβει αντίγραφα των πρωτότυπων μηνυμάτων ηλεκτρονικού ταχυδρομείου με συνημμένα αρχεία.

Με επιχειρηματικούς όρους

Φανταστείτε δύο περιπτώσεις στις οποίες ανοίγετε ένα έγγραφο από ένα συνημμένο μήνυμα ηλεκτρονικού ταχυδρομείου και αυτό:

01 Απλώς ανοίγει.

02 Εκτελεί μια μακροεντολή που στέλνει δεδομένα από τον φορητό σας υπολογιστή ή κρυπτογραφεί άλλα έγγραφα. Και τα δύο έγγραφα μπορεί να είναι πανομοιότυπα εξωτερικά, αλλά συμπεριφέρονται διαφορετικά.

Η υπηρεσία ηλεκτρονικού ταχυδρομείου της Microsoft ελέγχει τη συμπεριφορά του εγγράφου πριν το μήνυμα ηλεκτρονικού ταχυδρομείου φτάσει στο γραμματοκιβώτιό σας. Εάν η συμπεριφορά του είναι παρόμοια με το δεύτερο σενάριο, το μήνυμα ηλεκτρονικού ταχυδρομείου θα παραδοθεί χωρίς το συνημμένο.

Κανένας κρυπτογραφητής δεν θα διαπεράσει το εταιρικό ηλεκτρονικό ταχυδρομείο. Το σύστημα, σε αντίθεση με τους υπαλλήλους, δεν εμπιστεύεται τα παραπλανητικά μηνύματα ηλεκτρονικού ταχυδρομείου και τα διαγράφει αμέσως.

Απειλή

Κακόβουλοι σύνδεσμοι σε μηνύματα ηλεκτρονικού ταχυδρομείου

Λύση

Microsoft 365: Ασφαλείς σύνδεσμοι

Προφίλ και ρύθμιση παραμέτρων των ασφαλών συνδέσμων Office 365 ATP

Με όρους πληροφορικής

Κάθε κλικ από ένα μήνυμα ηλεκτρονικού ταχυδρομείου ή έγγραφο του Office ελέγχεται όταν ο χρήστης κάνει κλικ σε αυτό. Εάν ο σύνδεσμος οδηγεί σε κακόβουλη τοποθεσία, ο σύνδεσμος θα αποκλειστεί.

Ο διαχειριστής μπορεί να προσθέσει μη αυτόματα τοποθεσίες στις λίστες κακόβουλων τοποθεσιών.

Με επιχειρηματικούς όρους

Οι άνθρωποι που σήμερα αποκαλούμε "εισβολείς" έγιναν ειδικοί του μάρκετινγκ πριν από πολύ καιρό.

Στέλνουν ελκυστικά μηνύματα ηλεκτρονικού ταχυδρομείου, δημιουργούν αντίγραφα τραπεζικών ιστοσελίδων που μοιάζουν αληθινά και εκμεταλλεύονται τα ανθρώπινα συναισθήματα.

Το πάτημα ενός συνδέσμου σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου μπορεί να οδηγήσει σε επιδημία ιών ή σε απώλεια πρόσβασης σε μια τράπεζα, μια αγορά κ.λπ.

Οι πληροφορίες σχετικά με αυτούς τους συνδέσμους φτάνουν στη Microsoft μέσα σε λίγα λεπτά. Οι απόπειρες ανοίγματος τοποθεσιών με ιούς ή τοποθεσιών που προσποιούνται ότι είναι διαδικτυακές τράπεζες θα αποκλείονται.

Απειλή

Επιθέσεις ιών κρυπτογράφησης

Λύση

Windows 10: Ελεγχόμενη πρόσβαση σε φακέλους

Ρύθμιση παραμέτρων της ελεγχόμενης πρόσβασης σε φακέλους

Με όρους πληροφορικής

Η λειτουργία "Ελεγχόμενη πρόσβαση σε φακέλους" σάς επιτρέπει να αποκλείετε τις μη αξιόπιστες διεργασίες από το να πραγματοποιούν εγγραφές σε φακέλους που έχετε ορίσει. Δεν θα επηρεαστούν διεργασίες όπως η Εξερεύνηση των Windows ή το MS Word, ενώ οι αλλαγές από άγνωστες διεργασίες θα αποκλειστούν.

Αυτή η δυνατότητα δεν λειτουργεί εάν έχει εγκατασταθεί πρόγραμμα προστασίας από ιούς τρίτων μερών.

Με επιχειρηματικούς όρους

Οι κρυπτογραφητές αποτελούν σοβαρό πρόβλημα και συχνά παρακάμπτουν την προστασία από ιούς. Ακόμα και αν ένα σύστημα είναι κρυπτογραφημένο, τα αρχεία σε προστατευμένους φακέλους παραμένουν ανέγγιχτα.

Ακόμα και αν η εφαρμογή προστασίας από ιούς αποτύχει να αντιμετωπίσει έναν ιό κρυπτογράφησης, τα έγγραφά σας θα παραμείνουν απολύτως ασφαλή.

Απειλή

Επιθέσεις ιών κρυπτογράφησης

Λύση

Microsoft 365: OneDrive για επιχειρήσεις

Ρύθμιση παραμέτρων του OneDrive για επιχειρήσεις στα Windows 10

Με όρους πληροφορικής

Εάν οι κρυπτογραφητές διεισδύσουν σε ένα σύστημα, δεν κρυπτογραφούν μόνο έγγραφα αλλά και τις αρχειοθήκες και επίσης διαγράφουν σκιώδη αντίγραφα.

Ρυθμίστε τα έγγραφά σας στα Windows 10 ώστε να συγχρονίζονται με τον χώρο αποθήκευσης στο cloud του OneDrive για επιχειρήσεις και θα μπορείτε να ανακτήσετε τα πάντα. Τα αρχεία θα συγχρονιστούν αμέσως αφού αποθηκευτούν σε έναν ειδικό κατάλογο.

Ένα πρόγραμμα-πελάτης για συγχρονισμό είναι ενσωματωμένο στα Windows 10 ή μπορεί να εγκατασταθεί στα Windows 7.

Η ελάχιστη διαθέσιμη χωρητικότητα αποθήκευσης είναι 1 TB ανά χρήστη.

Η ενσωματωμένη διαχείριση εκδόσεων σάς επιτρέπει να ανακτάτε όχι μόνο την τρέχουσα έκδοση ενός αρχείου αλλά και τα προηγούμενα αντίγραφά του.

Με επιχειρηματικούς όρους

Έχετε θελήσει ποτέ να τραβήξετε τα μαλλιά σας από απογοήτευση όταν ένα έγγραφο διαγράφηκε κατά λάθος ή υπήρξε μια επίθεση από ιό κρυπτογράφησης; Ή όταν διαγράψατε ένα τμήμα εγγράφου χωρίς να υπάρχει τρόπος να το επαναφέρετε;

Εκτός από τους ιούς κρυπτογράφησης, υπάρχουν χρήστες που διαγράφουν σημαντικά δεδομένα, είτε σκόπιμα είτε όχι.

Μπορείτε να αποθηκεύσετε αυτόματα αντίγραφα στο cloud. Θα αποθηκευτούν επίσης όλες οι προηγούμενες εκδόσεις των εγγράφων.

Εάν τα αρχεία έχουν κρυπτογραφηθεί, διαγραφεί ή τροποποιηθεί, θα αποκατασταθούν ανεξάρτητα από το πόσες αλλαγές έγιναν σε αυτά.

Απειλή

Λήψη πληροφοριών από δίσκο χωρίς κωδικό πρόσβασης

Λύση

Windows 10: Κρυπτογράφηση BitLocker

Τεκμηρίωση του BitLocker

Με όρους πληροφορικής

Γνωρίζετε πολύ καλά ότι μπορείτε να αποσπάσετε έναν σκληρό δίσκο και να τον συνδέσετε σε έναν άλλο υπολογιστή.

Ή να πραγματοποιήσετε εκκίνηση από ένα DVD και να αποκτήσετε πρόσβαση στο σύστημα αρχείων. Και στις δύο περιπτώσεις, δεν χρειάζεται να γνωρίζετε τον κωδικό πρόσβασης.

Και, φυσικά, τα αφαιρούμενα μέσα μπορούν να χαθούν εύκολα, αλλά η αξία των πληροφοριών είναι πολλές φορές μεγαλύτερη από το κόστος των μέσων.

Πρέπει να κρυπτογραφούμε τις μονάδες δίσκου. Όπως κάθε μέτρο ασφαλείας, αυτό προσθέτει κάποια ταλαιπωρία και κινδύνους.

Η σωστή ρύθμιση του Bitlocker ελαχιστοποιεί τους κινδύνους.

Μπορείτε να αποθηκεύσετε κλειδιά ανάκτησης στην τοπική υπηρεσία καταλόγου Active Directory ή στο Azure Active Directory και να έχετε τη δυνατότητα ανάκτησης δεδομένων ακόμη και αν ο δίσκος έχει υποστεί φυσική βλάβη.

Για μεγαλύτερη αξιοπιστία, είναι λογικό να αρχειοθετήσετε τα δεδομένα.

Με επιχειρηματικούς όρους

Σήμερα, ο ευκολότερος τρόπος για να χάσετε πληροφορίες είναι να τις χάσετε μαζί με τη συσκευή.

Ο φορητός σας υπολογιστής που ξεχάστηκε στον έλεγχο του αεροδρομίου, μια μονάδα δίσκου flash που έπεσε από την τσάντα σας. Αυτές οι καταστάσεις δεν συνεπάγονται μόνο τα έξοδα αγοράς μιας νέας συσκευής, αλλά ενέχουν επίσης σοβαρούς κινδύνους μη εξουσιοδοτημένης πρόσβασης σε πληροφορίες.

Ακόμη και αν ο φορητός σας υπολογιστής προστατεύεται με κωδικό πρόσβασης, αυτό δεν θα εμποδίσει έναν επαγγελματία πληροφορικής να ανακτήσει πληροφορίες από αυτόν. Σε αυτούς τους φορητούς υπολογιστές, δεν είναι ασυνήθιστο να βρεθούν έγγραφα με λίστα κωδικών πρόσβασης ή να βρεθούν κωδικοί πρόσβασης αποθηκευμένοι σε ένα πρόγραμμα περιήγησης.

Κρυπτογραφήστε δίσκους και μονάδες flash με σημαντικά δεδομένα. Θα εξακολουθεί να είναι ενοχλητικό αν η συσκευή σας χαθεί ή κλαπεί, αλλά κανείς δεν θα μπορεί να έχει πρόσβαση στα δεδομένα.

Ακόμη και η απώλεια ενός υπολογιστή ή μιας μονάδας flash με σημαντικά δεδομένα δεν θα οδηγήσει σε καταστροφική διαρροή δεδομένων. Τα δεδομένα θα είναι ασφαλώς κρυπτογραφημένα και απρόσιτα στα αδιάκριτα μάτια.

Απειλή

Επιθέσεις σε κινητές συσκευές

Λύση

Microsoft Endpoint Manager (πρώην Microsoft Intune)

Τεκμηρίωση του Microsoft Intune

Με όρους πληροφορικής

Το Microsoft Intune μπορεί να διαχειρίζεται συσκευές από το cloud, οπότε είναι δυνατή η εκτέλεση λειτουργιών διαχείρισης ανεξάρτητα από την τοποθεσία του χρήστη.

Οι συσκευές μπορούν να διαμορφωθούν με την επιβολή παραμέτρων ώστε να ακολουθούν τις πολιτικές ασφαλείας, καθώς και να διαγράφουν ορισμένα δεδομένα ή όλα τα δεδομένα κατά τη λήξη της απασχόλησης.

Με επιχειρηματικούς όρους

Η Symantec πραγματοποίησε το ακόλουθο πείραμα: Αρκετά κινητά τηλέφωνα "ξεχάστηκαν κατά λάθος" σε δημόσιους χώρους στις ΗΠΑ και τον Καναδά. Το λογισμικό που ήταν εγκατεστημένο σε αυτά τα τηλέφωνα παρακολουθούσε όλες τις δραστηριότητες που εκτελούνταν με τις συσκευές.

Το 60% όσων βρήκαν τα τηλέφωνα δεν επιχείρησαν να τα επιστρέψουν. Μέσα σε λίγες ώρες, ο νέος ιδιοκτήτης θα άρχιζε να περιηγείται σε έγγραφα και φωτογραφίες και να ανοίγει εφαρμογές.

Η μεγαλύτερη απειλή που σχετίζεται με τις κινητές συσκευές είναι το γεγονός ότι οι συσκευές είναι προσωπικές, ενώ οι πληροφορίες που περιέχουν μπορεί να είναι εταιρικές. Οι διαθέσιμες επιλογές για τη διαχείριση προσωπικών συσκευών είναι μάλλον περιορισμένες.

Οι χρήστες είναι αρκετά απρόσεκτοι με τις προσωπικές τους συσκευές: δεν είναι κρυπτογραφημένες, συχνά δεν προστατεύονται από κωδικούς PIN, έχουν εγκατασταθεί αμφισβητήσιμες εφαρμογές και μπορούν να χαθούν. Επίσης, ένας πρώην υπάλληλος μπορεί να αποθηκεύσει ένα αρχείο αλληλογραφίας ή επαφές πελατών στο smartphone του.

Εάν οι υπάλληλοι της εταιρείας χειρίζονται εταιρική αλληλογραφία ή έγγραφα από τα κινητά τους τηλέφωνα, θα πρέπει να έχετε τη δυνατότητα να προστατεύετε τα εταιρικά δεδομένα.

Η σύνδεση των κινητών τηλεφώνων με την υπηρεσία MEM θα επιτρέψει την ασφαλέστερη διαμόρφωση των τηλεφώνων των εργαζομένων, καθώς και τη διαγραφή των επαγγελματικών δεδομένων (ή όλων των δεδομένων) κατά τη λήξη της απασχόλησης.

Η εταιρική αλληλογραφία και τα επαγγελματικά έγγραφα που είναι αποθηκευμένα σε ένα προσωπικό smartphone δεν θα "φύγουν" μαζί με τον πρώην εργαζόμενο. Σε περίπτωση κλοπής ή απώλειας, τα δεδομένα μπορούν να διαγραφούν από τη συσκευή εξ αποστάσεως.

Απειλή

Ιοί

Λύση

Windows 10: Microsoft Defender AV

Με όρους πληροφορικής

Εφαρμογή προστασίας από ιούς ενσωματωμένη στην πλατφόρμα των Windows 10. Η εφαρμογή προστασίας από ιούς Microsoft Security Essentials που χρησιμοποιούνταν στις προηγούμενες εκδόσεις ήταν αρκετά απλή. Το Microsoft Defender AV, ο διάδοχος του Security Essentials, διαφέρει ριζικά από τον προκάτοχό του.

Το βασικό πλεονέκτημα είναι η ενσωμάτωσή του στα Windows 10 και οι βελτιώσεις της ροής εργασιών με κάθε νέα έκδοση των Windows 10.

Η πρόοδος της ανάπτυξης των εφαρμογών προστασίας από ιούς εκπλήσσει ακόμη και τους ανεξάρτητους δοκιμαστές. Έκπληξη! Το Windows Defender δεν τα πάει χάλια στις τελευταίες δοκιμές AV https://www.tomsguide.com/us/windows-defender-av-test,news-25524.html

Η εφαρμογή προστασίας από ιούς είναι απολύτως δωρεάν για εταιρική χρήση και μπορεί να ελεγχθεί μέσω πολιτικών ομάδας.

Ορισμένες λειτουργίες, όπως η κεντρική υποβολή αναφορών, απαιτούν εμπορικά εργαλεία.

Με επιχειρηματικούς όρους

Μια εφαρμογή προστασίας από ιούς δεν είναι πανάκεια. Τα θέματα ασφάλειας δεν θα πρέπει να μένουν χωρίς παρακολούθηση, αλλά θα πρέπει να χρησιμοποιείται μια εφαρμογή προστασίας από ιούς. Είναι ενσωματωμένη και δωρεάν.

Παλαιότερα, τα Mac θεωρούνταν ασφαλέστερο περιβάλλον εργασίας από τα Windows, επειδή είχαν λιγότερους ιούς. Ο κύριος λόγος είναι ότι τα Windows έχουν το 88% της αγοράς συγκριτικά με το 9% των Mac (https://netmarketshare.com/operating-system-market-share.aspx)

Αυτοί που κερδίζουν χρήματα από τις εισβολές προφανώς εστιάζουν τις προσπάθειές τους στο μεγαλύτερο κοινό-στόχο. Χρησιμοποιώντας τα Windows 10 παραμένετε εντός του 88% και ταυτόχρονα είστε τόσο προστατευμένοι όσο και το 9%.

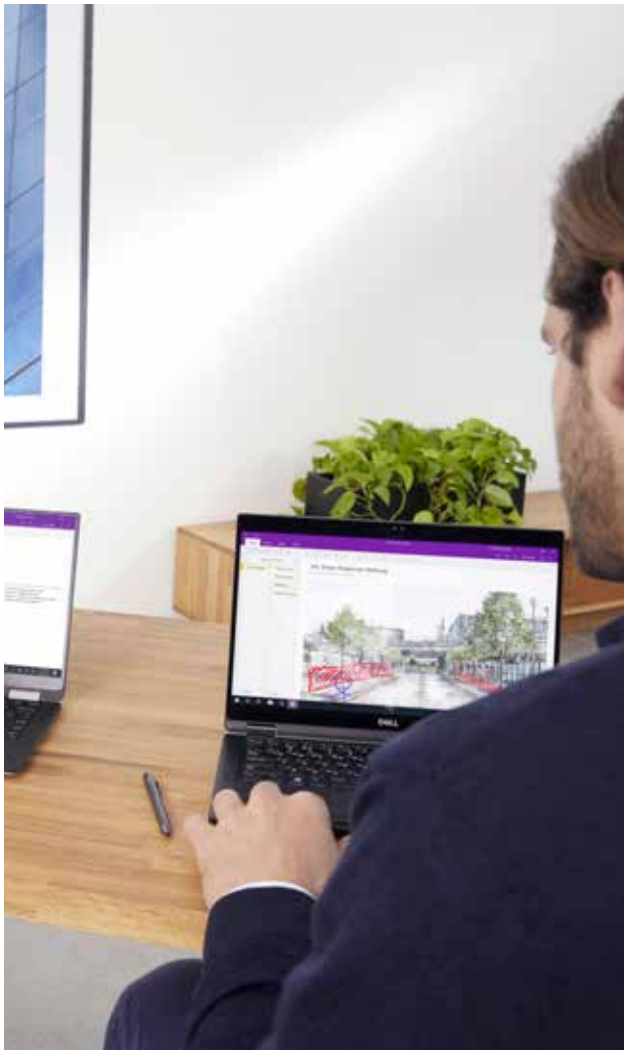
Απειλή

Διαρροή εγγράφων

Λύση

Προστασία πληροφοριών Azure

Τεκμηρίωση της Προστασίας πληροφοριών Azure



Με όρους πληροφορικής

Αυτή η τεχνολογία προστατεύει τα έγγραφα μέσω κρυπτογράφησης και εκχώρησης δικαιωμάτων πρόσβασης σε άλλους χρήστες, γεγονός που καθιστά δυνατή τη διατήρηση των διαμορφωμένων περιορισμών ακόμη και αν τα έγγραφα διαρρεύσουν εκτός της εταιρείας.

Η τεχνολογία συμβάλλει στη διαφύλαξη των εμπιστευτικών πληροφοριών εντός της εταιρείας και στην αποφυγή διαρροών δεδομένων.

Ενσωματώνεται σε εφαρμογές του Office, γεγονός που επιτρέπει στους χρήστες να κρυπτογραφούν αρχεία απευθείας από το Microsoft Word και με την αλληλογραφία του Microsoft Exchange. Έτσι, μπορεί να χρησιμοποιηθεί τόσο μη αυτόματα όσο και αυτόματα, σύμφωνα με καθορισμένους κανόνες. Για παράδειγμα, εάν ένας υπάλληλος στείλει ένα μήνυμα με συνημμένο αρχείο εκτός της εταιρείας/σε συγκεκριμένες διευθύνσεις/που περιέχει συγκεκριμένα αρχεία κ.λπ., το συνημμένο αρχείο μπορεί να κρυπτογραφηθεί αυτόματα.

Αυτή η τεχνολογία μπορεί να χρησιμοποιηθεί τόσο σε ένα σενάριο απλής περίπτωσης, όπου απαιτείται απλώς η εγκατάσταση προστασίας εγγράφων, όσο και για πιο προηγμένες εργασίες όπου τα έγγραφα προ-ταξινομούνται για να πληρούν τις απαιτήσεις των ρυθμιστικών αρχών και στη συνέχεια προστατεύονται.

Με επιχειρηματικούς όρους

Αυτή η τεχνολογία αξίζει πλήρως την επένδυση αν αναλογιστεί κανείς την αξία των εταιρικών δεδομένων που χρειάζονται προστασία. Ακόμη και αν κάποιος προσπαθήσει να μετακινήσει εμπιστευτικές πληροφορίες εκτός της εταιρείας, απλώς δεν θα μπορέσει να ανοίξει το έγγραφο.

Εάν ένας διευθυντής θελήσει να στείλει με email μια βάση δεδομένων πελατών σε ανταγωνιστές, η άλλη εταιρεία δεν θα είναι σε θέση να διαβάσει το email, όσο σκληρά και αν προσπαθήσει.

Τέλος, μπορείτε να περιορίσετε την πρόσβαση σε έγγραφα, ώστε να μην βλέπουν εξωτερικοί χρήστες πληροφορίες που δεν προορίζονται γι' αυτούς.

Απειλή

Περισσότερα για τη διαρροή

Λύση

Microsoft 365 DLP

Λεπτομερής επισκόπηση του Microsoft 365 DLP

Με όρους πληροφορικής

Ένα σύνολο πολιτικών προστασίας εμπιστευτικών πληροφοριών για το Exchange Online, το SharePoint Online, το OneDrive για επιχειρήσεις και το Teams.

Μια πολιτική μπορεί να απαγορεύσει μια σειρά από λειτουργίες για εμπιστευτικές πληροφορίες, όπως η προώθηση κάποιας πληροφορίας εκτός της εταιρείας ή η λήψη σε τοπικό υπολογιστή.

Οι διαχειριστές μπορούν να λαμβάνουν ειδοποιήσεις σχετικά με τις προσπάθειες των χρηστών να εκτελέσουν απαγορευμένες λειτουργίες.

Το σύστημα διατηρεί πρότυπα εμπιστευτικών πληροφοριών για τον εντοπισμό δεδομένων από ρωσικά εγχώρια και διεθνή διαβατήρια. Είναι επίσης δυνατή η ανάπτυξη προσαρμοσμένων προτύπων με βάση λέξεις-κλειδιά, κανονικές παραστάσεις, διατάξεις εγγράφων ή τάξεις με δυνατότητα εκπαίδευσης.

Με επιχειρηματικούς όρους

Η κυβέρνηση απαιτεί από τις εταιρείες να προστατεύουν τα προσωπικά δεδομένα από διαρροές.

Τι θα συνέβαινε αν ένας υπάλληλος έστελνε κατά λάθος ένα έγγραφο με στοιχεία διαβατηρίου;

Μια πραγματική υπόθεση: κατά τη διάρκεια της προετοιμασίας για τη σύνοδο κορυφής της G20 στο Μπρισμπέιν το 2015, ένας υπάλληλος του Αυστραλιανού Υπουργείου Μετανάστευσης έστειλε ακούσια ένα έγγραφο με τα στοιχεία διαβατηρίου των ηγετών χωρών της G20 (συμπεριλαμβανομένων των Πούτιν, Ομπάμα, Μέρκελ και Σι Τζινπίνγκ) στους διοργανωτές του τουρνουά του Ασιατικού Κυπέλλου Ποδοσφαίρου. Κατά την εισαγωγή της διεύθυνσης ενός συναδέλφου στο Outlook, αυτός ο υπάλληλος δεν έλεγξε τη διεύθυνση που προτάθηκε από τη λειτουργία αυτόματης συμπλήρωσης πριν από την αποστολή του μηνύματος.

Ο διαχειριστής σας μπορεί να ρυθμίσει μια πολιτική για τον αποκλεισμό εξερχόμενων μηνυμάτων ηλεκτρονικού ταχυδρομείου που περιέχουν στοιχεία διαβατήριων ή άλλα προσωπικά στοιχεία.

Απειλή

Και τι γίνεται με τις διαρροές μέσω του Teams;

Λύση

Microsoft 365 DLP για το Teams

Με όρους πληροφορικής

Η δυνατότητα DLP είναι διαθέσιμη για ηλεκτρονικό ταχυδρομείο, χώρους αποθήκευσης για το SharePoint / OneDrive για επιχειρήσεις και το Microsoft Teams.

Υπάρχουν βασικές διαφορές στην παραχώρηση αδειών χρήσης και το πεδίο εφαρμογής.

Στην περίπτωση του Microsoft Teams, οι πολιτικές θα ισχύουν για μηνύματα σε ιδιωτικές συνομιλίες και κανάλια.

Τα έγγραφα που δημοσιεύονται με τη βοήθεια του Microsoft Teams βρίσκονται στο OneDrive για επιχειρήσεις και στο SharePoint. Κατά συνέπεια, τα έγγραφα θα εμπίπτουν στο πεδίο εφαρμογής των πολιτικών DLP για το OneDrive για επιχειρήσεις και το SharePoint.

Με επιχειρηματικούς όρους

Η δημοτικότητα και η ευελιξία της υπηρεσίας Microsoft Teams φέρνει μαζί της πολλά πλεονεκτήματα αλλά και νέες προκλήσεις. Για παράδειγμα:

01 Ένας από τους υπαλλήλους σας προσκάλεσε έναν εκπρόσωπο μιας συνεργαζόμενης εταιρείας σε ένα κανάλι του Teams και έστειλε κατά λάθος εμπιστευτικά δεδομένα σε ένα μήνυμα.

02 Ένας υπάλληλος δημοσίευσε ένα έγγραφο που περιέχει εμπιστευτικά δεδομένα σε αυτό το κανάλι του Teams.

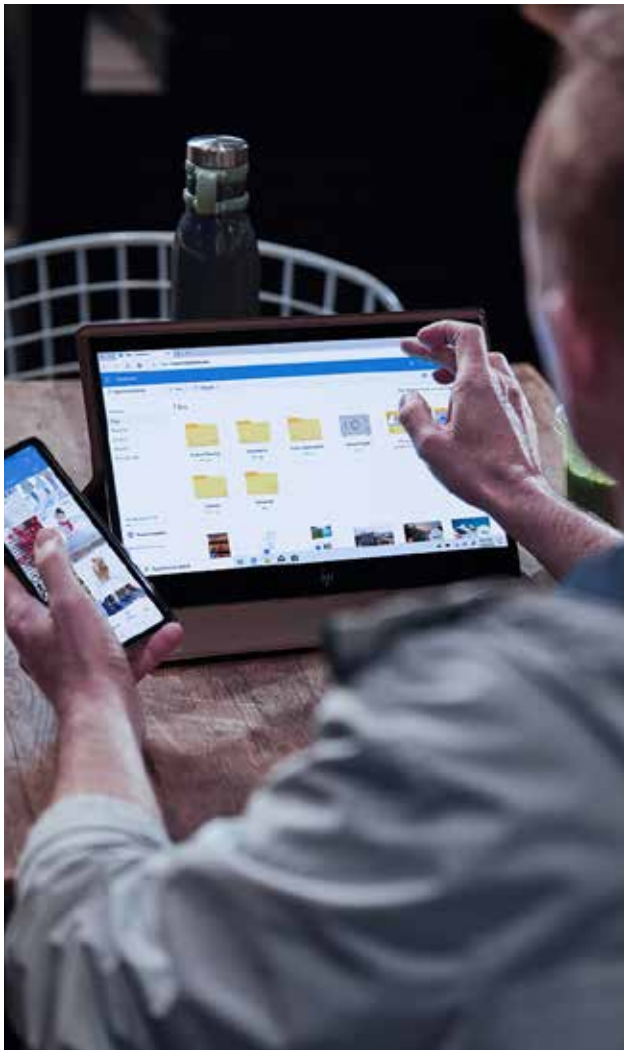
Και στις δύο περιπτώσεις, το μήνυμα και το έγγραφο δεν θα είναι διαθέσιμα στον εκπρόσωπο της συνεργαζόμενης εταιρείας και οι εμπιστευτικές πληροφορίες δεν θα βγουν από την εταιρεία.

Απειλή

Λίγες περισσότερες πληροφορίες για τις διαρροές και το shadow IT

Λύση

Office 365 Cloud App Security



Με όρους πληροφορικής

Το Microsoft Cloud App Security ανήκει στην οικογένεια Cloud Access Security Broker. Η λειτουργικότητα του Microsoft CAS είναι τόσο εκτεταμένη που αξίζει ένα ξεχωριστό βιβλίο. Ωστόσο, έχει έναν "μικρό αδελφό", το Office 365 CAS, το οποίο είναι υπεύθυνο μόνο για εφαρμογές και άλλα στοιχεία του Office 365.

Το Office 365 CAS μπορεί να παρακολουθεί τις δραστηριότητες των χρηστών στο Exchange Online, το SharePoint Online και το OneDrive για επιχειρήσεις. Για παράδειγμα, είναι δυνατό να μάθετε ποιος υπάλληλος έχει κατεβάσει ένα συγκεκριμένο αρχείο, έχει δημιουργήσει έναν ανώνυμο σύνδεσμο, έχει διαγράψει ένα μήνυμα ηλεκτρονικού ταχυδρομείου και ούτω καθεξής.

Οι δραστηριότητες των διαχειριστών θα καταγράφονται και μπορούν επίσης να εντοπιστούν.

Μπορούν να χρησιμοποιηθούν πολιτικές για την ειδοποίηση για συγκεκριμένες δραστηριότητες ή ακόμα και για την απενεργοποίησή τους.

Με επιχειρηματικούς όρους

Φανταστείτε ότι ένας υπάλληλος που αποχωρεί από την εταιρεία αποφάσισε να κατεβάσει ορισμένα έγγραφα που είναι σημαντικά για την εταιρεία (και τους ανταγωνιστές της).

Εάν αυτή η πρόθεση ανακαλυφθεί εγκαίρως, μπορεί να αντιμετωπιστεί. Μπορεί να ανακαλυφθεί με τη βοήθεια πολιτικών. Για παράδειγμα:

01 Ένας υπάλληλος έχει κατεβάσει 30 έγγραφα μέσα σε ένα λεπτό.

02 Ένας υπάλληλος έχει κατεβάσει 10 έγγραφα που έχουν επισημανθεί ως εμπιστευτικά.

03 Ένας υπάλληλος έχει δημιουργήσει έναν ανώνυμο σύνδεσμο για τη λήψη εμπιστευτικών εγγράφων... Και ούτω καθεξής.

Απειλή

Φυσική ασφάλεια

Λύση

Χρήση κέντρου δεδομένων

Με όρους πληροφορικής

Η ασφάλεια υποδομής συνδυάζει διάφορους παράγοντες, συμπεριλαμβανομένης της φυσικής ασφάλειας. Όταν ο εξοπλισμός βρίσκεται στις εγκαταστάσεις της εταιρείας, η διασφάλιση της φυσικής ασφάλειας μπορεί να μην είναι ασήμαντο έργο.

Ορισμένες σχετικές πτυχές που πρέπει να ληφθούν υπόψη:

01 Απαιτείται σωστή τοποθεσία για την αίθουσα διακομιστών. Συγκεκριμένα, οι τοίχοι της αίθουσας διακομιστών δεν πρέπει να γειτνιάζουν με τους εξωτερικούς τοίχους ή να έχουν παράθυρα.

02 Πρέπει να υπάρχει σύστημα για τη διατήρηση των παραμέτρων θερμοκρασίας και υγρασίας εντός των καθορισμένων ορίων.

03 Οι πόρτες πρέπει να είναι εξοπλισμένες με ηλεκτρονικές κλειδαριές.

04 Το κέντρο δεδομένων πρέπει να έχει ανυψωμένους ορόφους.

05 Το κέντρο δεδομένων πρέπει να διαθέτει σύστημα πυρόσβεσης.

06 Τα συστήματα υλικού και αποθήκευσης πρέπει να κρυπτογραφούνται.

07 Πρέπει να διασφαλιστεί η συνολική φυσική ασφάλεια των κτιρίων.

Οι ιδιοκτήτες των κέντρων δεδομένων έχουν ήδη προβεί σε προβλέψεις για όλα τα παραπάνω. Από την άποψη της ασφάλειας, τα δεδομένα σας θα προστατεύονται πολύ καλύτερα σε ένα μέρος που έχει όλα όσα απαιτούνται για τον σκοπό αυτό.

Με επιχειρηματικούς όρους

Όταν όλα τα δεδομένα βρίσκονται κοντά, υπάρχει φυσικά περισσότερη ηρεμία. Ωστόσο, όσοι μπορούν νόμιμα ή παράνομα να εισέλθουν στο έδαφος της εταιρείας μπορούν επίσης να πάρουν στην κατοχή τους τα δεδομένα σας. Δεν χρειάζεται καν να είναι εισβολείς. Μπορούν απλώς να πάρουν τον εξοπλισμό μαζί τους.

Τα κέντρα δεδομένων διαθέτουν συστήματα ελέγχου πρόσβασης, έλεγχο διέλευσης, παρακολούθηση βίντεο όλο το εικοσιτετράωρο και φύλακες ασφαλείας. Η πρόσβαση τρίτων μερών είναι μια περίπλοκη ή σχεδόν αδύνατη εργασία, ειδικά εάν το κέντρο δεδομένων όπου αποθηκεύονται τα δεδομένα σας βρίσκεται σε άλλη χώρα.

Οι μικρότερες εταιρείες δεν μπορούν συνήθως να αντέξουν οικονομικά μόνες τους αυτό το επίπεδο ασφάλειας, την προστασία των διακομιστών εσωτερικής εγκατάστασης, τον έλεγχο πρόσβασης και την παρακολούθηση βίντεο των διακομιστών.

Απειλή

Αρχειοθέτηση δεδομένων

Λύση

Αντίγραφο ασφαλείας σε κέντρο δεδομένων

Τεκμηρίωση της Δημιουργίας αντιγράφων ασφαλείας Azure

Με όρους πληροφορικής

Το εργαλείο δημιουργίας αντιγράφων ασφαλείας δεδομένων του Microsoft Azure είναι μια βασική λύση αρχειοθέτησης και αποκατάστασης δεδομένων που συμπληρώνει τα υπάρχοντα εργαλεία αρχειοθέτησης.

Ακόμα και αν ένα τοπικό αρχείο χαθεί ή καταστραφεί, θα διατηρείται ένα αντίγραφο ασφαλείας στο κέντρο δεδομένων Azure για όσο χρονικό διάστημα επιθυμείτε.

Με επιχειρηματικούς όρους

Ο εξοπλισμός μπορεί να παρουσιάσει αστοχία υλικού και τα δεδομένα μπορούν να διαγραφούν κατά λάθος ή σκόπιμα. Ένα αντίγραφο ασφαλείας μπορεί να σώσει μια τέτοια κατάσταση.

Κι αν το αντίγραφο καταστράφηκε κι αυτό; Αυτό θα μπορούσε να είναι αποτέλεσμα πυρκαγιάς, ληστείας ή απλώς απρόσεκτης αποθήκευσης μέσων.

Πιθανόν να ξέρετε την ταινία κινουμένων σχεδίων "Toy Story 2". Αλλά ξέρατε ότι τα περισσότερα πλάνα καταστράφηκαν ακούσια και η αποκατάσταση του αρχείου απέτυχε λόγω απρόσεκτης αποθήκευσης; Η ταινία ευτυχώς σώθηκε επειδή ένα μέλος της ομάδας είχε αντιγράψει τα πλάνα λίγο πριν από αυτό το περιστατικό και τα πήρε μαζί του για να εργαστεί από το σπίτι.

Η διασφάλιση αξιόπιστης αποθήκευσης αρχείων έχει υψηλό κόστος. Και ακόμη και οι κατάλληλες ρυθμίσεις αποθήκευσης μπορεί να αποτύχουν λόγω ανθρώπινου λάθους.
Ένα μεγάλο νοσοκομείο με έδρα τη Γιούτα αποθήκευσε τις αρχειοθήκες του με αρχεία ασθενών σε μια ασφαλή θυρίδα. Κάθε μέρα, ένας ταχυμεταφορέας παραλάμβανε τα δεδομένα και τα πήγαινε στη θυρίδα. Μια μέρα, πριν από το Σαββατοκύριακο, ο ταχυμεταφορέας αποφάσισε να μην παραδώσει τα δεδομένα την ίδια μέρα και άφησε το κουτί στο αυτοκίνητο το βράδυ. Κατά τη διάρκεια της νύχτας, το αυτοκίνητο παραβιάστηκε και τα δεδομένα εκλάπησαν. Η εταιρεία τελικά έπρεπε να πληρώσει εκατομμύρια δολάρια στους ασθενείς της.

Ο χώρος αποθήκευσης στο cloud είναι αξιόπιστος από τεχνολογική άποψη και δεν είναι ευάλωτος σε ανθρώπινες ελλείψεις.

Οποιαδήποτε δεδομένα, συμπεριλαμβανομένης μιας ετήσιας λογιστικής έκθεσης ή μιας βάσης δεδομένων μισθοδοσίας, μπορούν να ανακτηθούν ακόμη και μετά από σκόπιμη διαγραφή ή κατάργηση.

Απειλή

Εάν, παρ' όλα αυτά, πραγματοποιηθεί εισβολή

Λύση

Advanced Threat Analytics (τοπικά)
Το Microsoft Defender για ταυτότητα (πρώην Προηγμένη προστασία από απειλές του Azure) (βασισμένο στο cloud)
Τεκμηρίωση του Microsoft Defender για ταυτότητα

Με όρους πληροφορικής

Καμία προστασία δεν είναι 100% εγγυημένη. Το πρόβλημα είναι ότι οι εταιρείες συνήθως εντοπίζουν μια εισβολή λίγους μήνες μετά το περιστατικό, όταν ο εισβολέας έχει ήδη αποκτήσει όλα τα δεδομένα. Για να αποφευχθεί αυτό, απαιτείται τόσο προστασία όσο και παρακολούθηση.

Συνήθως, αυτή η λειτουργία πραγματοποιούνταν από IDS (Συστήματα Ανίχνευσης Εισβολής), αλλά τα συστήματα UBA (Ανάλυσης Συμπεριφοράς Χρηστών) είναι τα πιο πρόσφατα του είδους τους.

Τα UBA μελετούν συνέχεια ορισμένα χαρακτηριστικά συμπεριφοράς των εργαζομένων: πότε εργάζονται, σε ποιες συσκευές συνδέονται, σε ποια αρχεία αποκτούν πρόσβαση, σε ποιες ομάδες ανήκουν κ.λπ. Αφού δημιουργηθεί το προφίλ συμπεριφοράς ενός χρήστη, το σύστημα θα αναφέρει αποκλίσεις στη συμπεριφορά, οι οποίες θα μπορούσαν να είναι οι δραστηριότητες ενός υπαλλήλου-κατασκόπου ή ενός εισβολέα που έχει παραβιάσει έναν λογαριασμό χρήστη.

Το σύστημα UBA μπορεί να υλοποιηθεί με δύο διαφορετικούς τρόπους:

01 Μπορεί να εγκατασταθεί τοπικά και να αναλύει την κυκλοφορία της υπηρεσίας καταλόγου Active Directory. Αυτή η επιλογή ονομάζεται Microsoft ATA.

02 Μπορεί να βασίζεται στο cloud, με παράγοντες εγκατεστημένους τοπικά σε ελεγκτές τομέα. Αυτή η επιλογή ονομάζεται Microsoft Defender για ταυτότητα.

Με επιχειρηματικούς όρους

Καμία προστασία δεν είναι 100% εγγυημένη. Είναι ιδιαίτερα δύσκολη η προστασία από εκείνους που θεωρούνται εγγενώς αξιόπιστοι: τους εργαζομένους. Κανείς δεν μπορεί να εγγυηθεί ότι ένας εργαζόμενος που δεν πήρε ένα μπόνους δεν θα προβεί σε πράξη δολιοφθοράς ή αντιγραφής δεδομένων. Το σύστημα ανάλυσης συμπεριφοράς υπαλλήλων θα σας βοηθήσει να εντοπίσετε μη τυπικές συμπεριφορές.

Εάν ένας εργαζόμενος μείνει μετά το πέρας του ωραρίου για να εκτυπώσει εμπιστευτικά δεδομένα, το σύστημα θα εκδώσει σχετική ειδοποίηση.

Επίσης, το σύστημα παρέχει μια ειδοποίηση εάν ένας εργαζόμενος προσπαθήσει να αποκτήσει πρόσβαση σε έγγραφα που συνήθως δεν απαιτούνται για την εκτέλεση των καθηκόντων του.

Απειλή

Εάν, παρ' όλα αυτά, πραγματοποιηθεί εισβολή ή δεν έχει συμβεί ακόμα

Λύση

Microsoft Defender για τελικό σημείο

Οι περισσότερες κακόβουλες δραστηριότητες πραγματοποιούνται από εισβολείς σε σταθμούς εργασίας και διακομιστές. Για παράδειγμα, εάν υπήρξε παραβίαση ενός χρήστη μέσω μηνύματος email ηλεκτρονικού "ψαρέματος", ο εισβολέας μπορεί να αποκτήσει πρόσβαση στον σταθμό εργασίας του και να συνδεθεί με άλλους από εκεί.

Οι σταθμοί εργασίας προστατεύονται από προεπιλογή από λογισμικό προστασίας από ιούς, αλλά οι δυνατότητες των λογισμικών προστασίας από ιούς είναι περιορισμένες. Αυτό το λογισμικό βασίζεται στους πόρους του σταθμού εργασίας και ο εντοπισμός προηγμένων επιθέσεων μπορεί να δυσχεράνει σοβαρά τη λειτουργία του υπολογιστή.

Ο εντοπισμός και ο αποκλεισμός μπορούν να μεταφερθούν στο cloud. Σε αυτήν την περίπτωση, μια ενσωματωμένη υπηρεσία θα μεταδίδει συμβάντα υπολογιστή στην υπηρεσία cloud, όπου θα αναλύονται με τη χρήση τεχνητής νοημοσύνης και της γνωσιακής βάσης της Microsoft.

Εάν η εταιρεία διαθέτει Κέντρο Επιχειρήσεων Ασφαλείας (SOC), η διερεύνηση περιστατικών είναι πολύ πιο εύκολη.

Απειλή

Παραβίαση ενός χρήστη με δικαιώματα διαχείρισης

Λύση

Azure AD Privileged Identity Management

Μία από τις βασικές αρχές μιας ασφαλούς ανάθεσης δικαιωμάτων σε μια τοπική υπηρεσία καταλόγου Active Directory είναι ότι ο διαχειριστής θα πρέπει να έχει διάφορους λογαριασμούς με διαφορετικά δικαιώματα. Για παράδειγμα:

01 Ένας λογαριασμός χωρίς δικαιώματα δραστηριότητας στο Internet

02 Ένας λογαριασμός για τη διαχείριση σταθμού εργασίας

03 Ένας λογαριασμός για τη διαχείριση διακομιστή

04 Ένας λογαριασμός για τη διαχείριση τομέα

05 Κ.λπ.

Ακόμα και αν ένας από τους λογαριασμούς υποστεί παραβίαση, ο εισβολέας δεν θα αποκτήσει όλα τα σχετικά δικαιώματα.
Δυστυχώς, λόγω της αναστάτωσης από την εναλλαγή μεταξύ πολλαπλών λογαριασμών, ορισμένες εταιρείες παραμελούν αυτήν τη σύσταση.

Στο cloud, η χρήση ενός μόνο λογαριασμού με σημαντικό αριθμό δικαιωμάτων θα προκαλέσει παρόμοια προβλήματα.

Η δυνατότητα Azure AD PIM χρησιμεύει για να καταστήσει την ανάθεση δικαιωμάτων ασφαλή και ταυτόχρονα να αποτρέψει την ύπαρξη πολλών λογαριασμών.
Με αυτήν τη λειτουργία, ο διαχειριστής θα έχει μόνο τα δικαιώματα ενός απλού χρήστη και άλλα δικαιώματα θα ενεργοποιούνται όταν απαιτείται.

Ένα παράδειγμα: ένας μηχανικός υποστήριξης πρέπει να επαναφέρει έναν κωδικό πρόσβασης χρήστη. Η διαδικασία θα μπορούσε να είναι ως εξής:

01 Ο μηχανικός συνδέεται και εντοπίζει τη δυνατότητα Azure AD PIM. Στη συνέχεια, κάνει κλικ στην επιλογή "Ενεργοποίηση του ρόλου Διαχειριστή υπηρεσίας βοήθειας".

02 Στη συνέχεια, υποβάλλεται σε πρόσθετο έλεγχο ταυτότητας με MFA.

03 Υποδεικνύει τον αριθμό των ωρών για τις οποίες θα διατηρηθούν ενεργά αυτά τα δικαιώματα.

04 Λαμβάνει έγκριση από τον αρμόδιο υπεύθυνο έγκρισης.

05 Μπορεί να χρησιμοποιήσει τα δικαιώματα διαχείρισης κατά τη διάρκεια του επιτρεπόμενου αριθμού ωρών.
Ακόμα και αν ο λογαριασμός παραβιαστεί, ο εισβολέας δεν θα έχει πρόσβαση με δικαιώματα διαχείρισης.

Αυτή η δυνατότητα υλοποιείται επίσης εν μέρει για την τοπική υπηρεσία καταλόγου Active Directory και ονομάζεται Privileged Access Management (PAM).

Συμπέρασμα

Με βάση το πεδίο εφαρμογής των απειλών και των μεθόδων προστασίας που περιγράφονται παραπάνω, μπορούμε να συμπεράνουμε ότι η ασφάλεια πρέπει να λαμβάνεται υπόψη ως μια ολοκληρωμένη προσέγγιση. Δεν υπάρχει ένα μαγικό κουμπί που θα πατήσετε για να αποκτήσετε καθολική προστασία. Ομοίως, δεν υπάρχει ένα προϊόν λογισμικού που να μπορεί να εγγυηθεί την ασφάλεια σε όλα τα επίπεδα. Για ευκολία και εξοικονόμηση κόστους, η Microsoft προσφέρει προϊόντα λογισμικού τόσο ως μεμονωμένα στοιχεία όσο και ως σουίτες. Η σουίτα που περιλαμβάνει την πλειοψηφία των δυνατοτήτων που περιγράφονται εδώ ονομάζεται Microsoft 365. Περισσότερες λεπτομέρειες σχετικά με τις τρέχουσες προσφορές για το Microsoft 365 είναι διαθέσιμες στην επίσημη τοποθεσία: https://www.microsoft.com/el-gr/microsoft-365


Microsoft