ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Οδηγός 15 σημείων
ενίσχυσης της κυβερνοασφάλειας και αποτροπής λυτρισμικών επιθέσεων (ransomware) για τα Πανεπιστημιακά Ιδρύματα

Οι εγνωσμένες πρακτικές που συντελούν στην προληπτική άμυνα στο ψηφιακό οικοσύστημα ελαχιστοποιούν τους κινδύνους λυτρισμικών επιθέσεων (ransomware) και προάγουν ένα ασφαλές ψηφιακό περιβάλλον στα Πανεπιστημιακά Ιδρύματα. Γνωρίστε τις απειλές και πώς αυτές μπορούν να προσβάλουν και να προκαλέσουν ζημία στα συστήματα της πανεπιστημιακής κοινότητας. Εφαρμόστε τον «Οδηγό» ενίσχυσης της κυβερνοασφάλειας που ακολουθεί θωρακίζοντας το οικείο ψηφιακό σας οικοσύστημα.

Λυτρισμικές επιθέσεις (ransomware): τύπος κυβερνοεπίθεσης κατά τον οποίο κακόβουλο λογισμικό διεισδύει σε έναν υπολογιστή ή δίκτυο, κρυπτογραφεί τα αρχεία και τα καθιστά απρόσιτα. Οι εισβολείς απαιτούν λύτρα (συνήθως σε κρυπτονομίσματα) προκειμένου να δοθεί το κλειδί αποκρυπτογράφησης και να αποκατασταθεί η πρόσβαση στα δεδομένα.

1. Αντίγραφα Ασφαλείας και Ανάκαμψης Δεδομένων

Γιατί – Τα τακτικά, offline, αντίγραφα ασφαλείας είναι απαραίτητα για την ανάκτηση από λυτρισμικές επιθέσεις. Επιτρέπουν στο πανεπιστημιακό ίδρυμα να αποκαταστήσει δεδομένα και να συνεχίσει τη λειτουργία του γρήγορα, μειώνοντας τον χρόνο διακοπής και την απώλεια δεδομένων αν τα συστήματα παραβιαστούν.

Πώς – Δημιουργήστε μια ρουτίνα για τη δημιουργία αντιγράφων ασφαλείας κρίσιμων δεδομένων, διασφαλίζοντας ότι τα αντίγραφα αποθηκεύονται offline ή σε ασφαλή, ξεχωριστά περιβάλλοντα για να αποτραπεί λυτρισμική επίθεση σε αυτά. Πραγματοποιείτε περιοδικά τη διαδικασία επαναφοράς, προκειμένου να επαληθεύσετε ότι η ανάκτηση δεδομένων μπορεί να ολοκληρωθεί εντός των απαιτούμενων χρονικών πλαισίων. Καταγράψτε και αναθεωρήστε τα βήματα

ανάκτησης με το προσωπικό πληροφορικής, ώστε να είναι έτοιμο να τα εκτελέσει υπό πίεση σε πραγματικό περιστατικό.

2. Καταγραφή Υλικού και Λογισμικού

Γιατί – Οι οργανισμοί δεν μπορούν να αμυνθούν αποτελεσματικά έναντι των κυβερνοαπειλών, εάν δεν γνωρίζουν με ακρίβεια τι αγαθά διαθέτουν. Επιπλέον, η καταγραφή και ορθή διαχείριση των πληροφοριακών αγαθών έχει ως αποτέλεσμα οι οργανισμοί να εντοπίσουν τα κρίσιμα δεδομένα τους, καθώς και τα συστήματα που επεξεργάζονται αυτά τα δεδομένα, έτσι ώστε να υλοποιηθούν τα κατάλληλα μέτρα ασφάλειας.

Πώς – Δημιουργήστε έναν ακριβή και ενημερωμένο κατάλογο των συσκευών (όπως servers, end-user workstations, network devices) και λογισμικού (λειτουργικά συστήματα και εφαρμογές) που βρίσκονται στην υποδομή σας, καθώς και σε cloud περιβάλλοντα. Διασφαλίστε ότι ο κατάλογος περιέχει λεπτομερή στοιχεία για κάθε αγαθό (asset name, owner, department, ip & mac address κ.α.). Για τη δημιουργία του καταλόγου, προτιμήστε αυτοματοποιημένα εργαλεία που εκτελούν σαρώσεις και εντοπίζουν συνδεδεμένες συσκευές στο δίκτυό σας, μαζί με τα χαρακτηριστικά τους.

3. Πολυπαραγοντικός Έλεγχος Ταυτότητας (MFA)

Γιατί – Το MFA (Πολυπαραγοντικός Έλεγχος Ταυτότητας) θωρακίζει την ασφάλεια πρόσβασης απαιτώντας ένα επιπλέον επίπεδο επαλήθευσης. Ακόμα και αν ένας κωδικός παραβιαστεί, το MFA συντελεί στην αποτροπή μη εξουσιοδοτημένης πρόσβασης, δυσχεραίνοντας την είσοδο εισβολέων σε κρίσιμα πεδία.

Πώς – Εφαρμόστε MFA στα κρίσιμα συστήματα, ειδικά σε σημεία υψηλού κινδύνου, όπως λογαριασμοί διοίκησης, διδακτικού προσωπικού και φοιτητών. Όπου είναι δυνατόν, διαμορφώστε το MFA για συστήματα με απομακρυσμένη πρόσβαση και για εφαρμογές που βασίζονται στο cloud. Για περιοχές όπου το MFA δεν είναι εφικτό, εφαρμόστε πρόσθετους ελέγχους, όπως λευκές λίστες IP ή κωδικούς μίας χρήσης, για να ενισχύσετε την ασφάλεια.

4. Τακτικές Αναβαθμίσεις Λογισμικού και Ενημερώσεις

Γιατί – Η τακτική ενημέρωση κλείνει τα κενά ενός παρωχημένου λογισμικού, καθιστώντας πιο δύσκολη την εισβολή των επιτιθέμενων σε δίκτυα. Οι λυτρισμικές επιθέσεις και άλλες μορφές κακόβουλου λογισμικού συχνά εκμεταλλεύονται αυτές τις ευπάθειες.

Πώς – Εγκαταστήστε ένα αυτοματοποιημένο σύστημα διαχείρισης ενημερώσεων προκειμένου να διασφαλίσετε ότι όλα τα λειτουργικά συστήματα, οι εφαρμογές λογισμικού και οι συσκευές δικτύου ενημερώνονται τακτικά. Προγραμματίστε χρόνο αδράνειας, αν χρειάζεται, για να εφαρμοστούν οι ενημερώσεις χωρίς να διαταράσσονται οι λειτουργίες του πανεπιστημίου. Χρησιμοποιήστε εργαλεία ανίχνευσης ευπαθειών για να εντοπίσετε και να προτεραιοποιήσετε ενημερώσεις για κρίσιμα και εκτεθειμένα συστήματα. Εφαρμόστε τις άμεσα προκειμένου να αποτρέψετε την εκμετάλλευσή τους.

5. Ανίχνευση και Ανταπόκριση σε Σημεία Τερματικών (EDR)

Γιατί – Το EDR (Ανίχνευση και Ανταπόκριση σε Σημεία Τερματικών) παρέχει σε πραγματικό χρόνο ορατότητα στις δραστηριότητες των τερματικών και συντελεί στη γρήγορη ανταπόκριση σε ύποπτες συμπεριφορές, περιορίζοντας έτσι τη μόλυνση από λυτρισμική επίθεση, πριν προλάβει να εξαπλωθεί και προκαλέσει εκτεταμένη ζημιά.

Πώς – Αναπτύξτε λύσεις EDR σε όλες τις ψηφιακές συσκευές του ιδρύματος, όπως επιτραπέζιους υπολογιστές, φορητούς υπολογιστές και διακομιστές. Βεβαιωθείτε ότι τα εργαλεία EDR είναι διαμορφωμένα ώστε να παρακολουθούν ύποπτες συμπεριφορές, όπως ασυνήθιστες αλλαγές αρχείων ή υψηλή χρήση CPU, που θα μπορούσαν να υποδηλώνουν λυτρισμική επίθεση. Το EDR θα πρέπει να περιλαμβάνει επίσης αυτοματοποιημένες δυνατότητες ανταπόκρισης για την απομόνωση των επηρεασμένων τερματικών γρήγορα αν ανιχνευτεί μόλυνση, αποτρέποντας τη διάδοσή της στο δίκτυο.

6. Εκπαίδευση Ευαισθητοποίησης για Phishing

Γιατί – Το phishing παραμένει κύρια μέθοδος λυτρισμικών επιθέσεων. Εκπαιδεύοντας τους χρήστες να αναγνωρίζουν και να αποφεύγουν τις προσπάθειες phishing, τα πανεπιστήμια μπορούν να μειώσουν τις πιθανότητες επιτυχούς λυτρισμικής επίθεσης που πηγάζει από ανθρώπινα λάθη.

Πώς – Διεξάγετε συνεχή εκπαίδευση για φοιτητές, διδακτικό προσωπικό και εργαζομένους ώστε να αναγνωρίζουν και να αναφέρουν προσπάθειες phishing. Χρησιμοποιήστε ρεαλιστικά παραδείγματα και διαδραστικές προσομοιώσεις για να ενισχύσετε την εκπαίδευση και βεβαιωθείτε ότι οι χρήστες γνωρίζουν πώς να χειρίζονται ύποπτα μηνύματα. Συμπεριλάβετε αυτήν την εκπαίδευση κατά την ένταξη νέων φοιτητών και εργαζομένων, και πραγματοποιήστε περιοδικές αξιολογήσεις για να μετρήσετε τη βελτίωση και να προσαρμόσετε τα θέματα εκπαίδευσης.

7. Κατακερματισμός Δικτύου (Network Segmentation)

Γιατί – Ο κατακερματισμός περιορίζει τη διάδοση λυτρισμικής επίθεσης, περιορίζοντάς το σε συγκεκριμένο τμήμα του δικτύου. Αυτό μειώνει την αντίδραση ντόμινο και καθιστά πιο εύκολη την απομόνωση των επηρεασμένων περιοχών κατά τη διάρκεια επίθεσης.

Πώς – Σχεδιάστε το δίκτυό σας με κατακερματισμό, ομαδοποιώντας τα συστήματα και τις συσκευές βάσει λειτουργιών (π.χ. φοιτητές, διδακτικό προσωπικό, έρευνα, διοίκηση). Χρησιμοποιήστε τείχη προστασίας (firewalls) και VLANs για να ελέγχετε τη ροή δεδομένων μεταξύ αυτών των τμημάτων, επιτρέποντας μόνο τις απαραίτητες συνδέσεις. Εφαρμόστε ελέγχους πρόσβασης και παρακολούθηση για να εντοπίζετε μη εξουσιοδοτημένες προσπάθειες κίνησης μεταξύ τμημάτων, μειώνοντας έτσι τον κίνδυνο λυτρισμικής επίθεσης σε όλα τα συστήματα αν παραβιαστεί ένα τμήμα.

8. Διαχείριση Προνομιακής Πρόσβασης (PAM)

Γιατί – Οι προνομιακοί λογαριασμοί (PAM) είναι ελκυστικοί στόχοι για λυτρισμικές επιθέσεις, καθώς επιτρέπουν ευρεία πρόσβαση στα συστήματα.

Περιορίζοντας και παρακολουθώντας τη χρήση τους, μειώνονται οι πιθανοί δρόμοι εισόδου και περιορίζεται η δυνατότητα διάδοσης των επιθέσεων αυτών.

Πώς – Επιβάλλετε πολιτικές ελάχιστης πρόσβασης, περιορίζοντας τη χρήση προνομιακών λογαριασμών σε απαραίτητο προσωπικό και εργασίες. Χρησιμοποιήστε λογισμικό PAM για τη διαχείριση και παρακολούθηση αυτών των λογαριασμών, διασφαλίζοντας ότι η πρόσβαση παρέχεται μόνο όταν είναι απαραίτητη. Απαιτήστε MFA για προνομιακούς λογαριασμούς και καταγράψτε όλες τις δραστηριότητες για να διατηρείτε ίχνη ελέγχου. Αναθεωρήστε και προσαρμόστε τακτικά τις άδειες πρόσβασης ώστε να ευθυγραμμίζονται με τους τρέχοντες ρόλους και ευθύνες.

9. Φιλτράρισμα Email και Ανίχνευση Απειλών

Γιατί – Το email είναι ένα κοινό σημείο εισόδου για λυτρισμικές επιθέσεις συχνά μέσω κακόβουλων συνδέσμων ή συνημμένων αρχείων. Το φιλτράρισμα και η ανίχνευση των email μειώνει τις πιθανότητες να φτάσουν αυτές οι απειλές στα εισερχόμενα των χρηστών, προσθέτοντας ένα ισχυρό στρώμα προληπτικής άμυνας.

Πώς – Ρυθμίστε προηγμένο φιλτράρισμα email με εργαλεία που υποστηρίζουν sandboxing, επιτρέποντας τον έλεγχο συνημμένων και συνδέσμων σε ένα ασφαλές περιβάλλον πριν φτάσουν στους χρήστες. Διαμορφώστε το σύστημα ώστε να μπλοκάρει ή να θέτει σε καραντίνα email από ύποπτους τομείς και προσθέστε ειδοποιήσεις για μηνύματα που περιέχουν γνωστούς κακόβουλους δείκτες. Εκπαιδεύστε τους χρήστες να αναφέρουν ύποπτα email στο τμήμα IT και εφαρμόστε διαδικασίες ταχείας ανταπόκρισης για τη διαχείριση περιστατικών phishing.

10. Ασφαλής Διαμόρφωση και Θωράκιση Συστημάτων

Γιατί – Οι εσφαλμένες ρυθμίσεις και οι περιττές υπηρεσίες δημιουργούν ευπάθειες που μπορεί να εκμεταλλευτούν οι λυτρισμικές επιθέσεις. Η περιχαράκωση των συστημάτων διασφαλίζει ότι είναι διαμορφωμένα με ασφάλεια, μειώνοντας τις πιθανότητες εκμετάλλευσής τους.

Πώς – Εφαρμόστε ασφαλή πρότυπα διαμόρφωσης σε διακομιστές, σταθμούς εργασίας και συσκευές δικτύου. Απενεργοποιήστε μη χρησιμοποιούμενες θύρες, αφαιρέστε περιττό λογισμικό και εφαρμόστε ισχυρές ρυθμίσεις ασφαλείας για εφαρμογές, ειδικά για συστήματα με ευαίσθητα δεδομένα. Διεξάγετε τακτικούς ελέγχους διαμόρφωσης και διορθώστε τυχόν αποκλίσεις από τα ασφαλή πρότυπα, αξιοποιώντας αυτοματοποιημένα εργαλεία συμμόρφωσης, όπου είναι δυνατόν προκειμένου να απλοποιήσετε αυτή τη διαδικασία.

11. Καταγραφή και Παρακολούθηση Συμβάντων (Event Logs)

Γιατί – Η συλλογή και ανάλυση των logs αποτελεί κρίσιμη παράμετρο για την ικανότητα του οργανισμού να ανιχνεύσει έγκαιρα κάποια κακόβουλη δραστηριότητα. Μερικές φορές, τα αρχεία καταγραφής συμβάντων αποτελούν το μοναδικό αποδεικτικό στοιχείο μίας επιτυχημένης κυβερνοεπίθεσης. Έχει παρατηρηθεί ότι εξ αιτίας ανεπαρκών ή ανύπαρκτων διαδικασιών ανάλυσης των logs, σε αρκετές περιπτώσεις οι επιτιθέμενοι είχαν αποκτήσει πρόσβαση και είχαν πλήρη έλεγχο των συστημάτων για μήνες ή χρόνια, χωρίς κανείς στον οργανισμό-στόχο να το γνωρίζει.

Πώς – Ενεργοποιήστε την καταγραφή των logs σε κρίσιμα συστήματα, καθώς και σε firewalls, proxies και remote access systems (VPN κ.λπ.). Ιδίως, ενεργοποιήστε την καταγραφή των access control logs κατά την απόπειρα πρόσβασης σε πόρους χωρίς τα απαραίτητα προνόμια. Συλλέγετε τα logs και προβείτε σε ανάλυσή τους σε εβδομαδιαία βάση, ή συχνότερα, με σκοπό την ανίχνευση δυνητικών απειλών. Στο μέτρο του εφικτού, υλοποιήστε εργαλείο SIEM (Security Information and Event Management), το οποίο συλλέγει logs από διάφορες πηγές, τα συσχετίζει και τα αναλύει αυτοματοποιημένα σε πραγματικό χρόνο, και παρέχει ειδοποιήσεις (alerts) για πιθανή κακόβουλη δραστηριότητα. Διασφαλίστε τον συγχρονισμό ανάμεσα στα ρολόγια όλων των συσκευών, έτσι ώστε να επιτυγχάνεται ακρίβεια στη συσχέτιση συμβάντων μεταξύ διαφορετικών συστημάτων.

12. Σχέδιο Απόκρισης σε Περιστατικά (Incident Response Plan)

Γιατί – Ένα σχέδιο IR (Απόκρισης Περιστατικού) επιτρέπει ταχεία και οργανωμένη δράση κατά τη διάρκεια ενός περιστατικού λυτρισμικής επίθεσης, βοηθώντας να περιοριστεί η ζημιά και να επιτευχθεί ταχύτερη ανάκαμψη. Η προετοιμασία είναι καθοριστική για τη μείωση των επιπτώσεων, διασφαλίζοντας ότι το προσωπικό γνωρίζει τους ρόλους του και είναι έτοιμο να ανταποκριθεί αποτελεσματικά.

Πώς – Αναπτύξτε ένα ολοκληρωμένο σχέδιο IR που περιγράφει συγκεκριμένες ενέργειες, ρόλους και ευθύνες για την ανταπόκριση σε λυτρισμικές επιθέσεις. Συμπεριλάβετε ένα σχέδιο επικοινωνίας για την ειδοποίηση των επηρεαζόμενων χρηστών, εξωτερικών ενδιαφερόμενων και των αρχών επιβολής του νόμου, αν είναι απαραίτητο. Διεξάγετε τακτικά ασκήσεις προσομοίωσης για να δοκιμάσετε το σχέδιο και να το προσαρμόσετε βάσει των συμπερασμάτων που αντλήθηκαν, διασφαλίζοντας ότι η ομάδα IR μπορεί να ενεργεί γρήγορα και αποτελεσματικά σε μια πραγματική επίθεση.

13. Αποφυγή Χρήσης Πειρατικού Λογισμικού

Γιατί – Το πειρατικό λογισμικό συχνά περιέχει ενσωματωμένο κακόβουλο λογισμικό, το οποίο προστίθεται σκόπιμα από επιτιθέμενους και μπορεί να τους παρέχει «κρυφή πρόσβαση» στα συστήματά σας. Αυτές οι «κρυφές προσβάσεις» πωλούνται συχνά στο σκοτεινό διαδίκτυο σε εγκληματικές οργανώσεις, επιτρέποντάς τους πρόσβαση στο δίκτυό σας και σε ευαίσθητα δεδομένα. Η χρήση νόμιμου, αδειοδοτημένου λογισμικού βοηθά στη διασφάλιση ότι το λογισμικό δεν έχει παραποιηθεί και μειώνει τον κίνδυνο ακούσιας εισαγωγής κακόβουλου λογισμικού.

Πώς – Εφαρμόστε αυστηρές πολιτικές που απαγορεύουν τη χρήση μη αδειοδοτημένου ή πειρατικού λογισμικού σε συσκευές και δίκτυα του πανεπιστημίου. Πραγματοποιήστε τακτικούς ελέγχους για να εντοπίσετε μη εξουσιοδοτημένο λογισμικό και εκπαιδεύστε φοιτητές, διδακτικό προσωπικό και εργαζομένους για τους κινδύνους που σχετίζονται με τα πειρατικά προγράμματα. Παρέχετε πρόσβαση σε αδειοδοτημένες εναλλακτικές λύσεις για να μειώσετε τον πειρασμό χρήσης πειρατικών εκδόσεων.

14. Παρακολούθηση για Μη Εξουσιοδοτημένο Crypto Mining, Tor και Υπηρεσίες Torrent

Γιατί – Η μη εξουσιοδοτημένη εξόρυξη κρυπτονομισμάτων και η μη κατάλληλη χρήση υπηρεσιών Tor και Torrent ενδέχεται να ενέχουν κινδύνους ασφαλείας και λειτουργικούς κινδύνους. Ωστόσο, η χρήση αυτών των πρωτοκόλλων για ακαδημαϊκούς ή συναφείς σκοπούς μπορεί να είναι απαραίτητη για την έρευνα, την ανάλυση δεδομένων ή άλλες εγκεκριμένες δραστηριότητες. Στις περιπτώσεις που τέτοιες δραστηριότητες είναι γνωστές ή προβλέπονται από την πολιτική του ιδρύματος, δεν θα πρέπει να αποκλείονται, αλλά να παρακολουθούνται για να διασφαλιστεί ότι χρησιμοποιούνται με τρόπο που δεν θέτει σε κίνδυνο την ασφάλεια ή τη λειτουργία του δικτύου.

Πώς – Πραγματοποιείτε τακτικές σαρώσεις στο πανεπιστημιακό δίκτυο για μη εξουσιοδοτημένο λογισμικό εξόρυξης κρυπτονομισμάτων και χρήση των υπηρεσιών Tor και Torrent. Διασφαλίστε ότι η παρακολούθηση λαμβάνει υπόψη την ενδεχόμενη ακαδημαϊκή ή άλλη σχετική χρήση, διαχωρίζοντας περιπτώσεις κακόβουλης ή μη εξουσιοδοτημένης δραστηριότητας από εγκεκριμένες ή προβλέψιμες χρήσεις. Χρησιμοποιήστε εργαλεία παρακολούθησης για την ανίχνευση ασυνήθιστων μοτίβων, όπως υπερβολική χρήση πόρων για crypto mining ή δραστηριότητα δικτύου που υποδηλώνει κακή χρήση. Ρυθμίστε πολιτικές και διαδικασίες που επιτρέπουν την ακαδημαϊκή χρήση υπό συγκεκριμένους όρους, όπως περιορισμένη πρόσβαση, κατάλληλες άδειες και παρακολούθηση για διατήρηση της ασφάλειας.

15. Υλοποίηση Ελέγχων Παρείσδυσης (Penetration Tests)

Γιατί – Στο σύγχρονο πολύπλοκο διεθνές οικοσύστημα, όπου οι τεχνολογίες μεταβάλλονται συνεχώς και νέες επιθετικές τεχνικές εμφανίζονται σε τακτική βάση, οι οργανισμοί θα πρέπει περιοδικά να αξιολογούν την αποτελεσματικότητα των μέτρων κυβερνοασφάλειας που έχουν υλοποιήσει, με σκοπό να εντοπίσουν κενά τα οποία οι επιτιθέμενοι μπορούν να εκμεταλλευτούν για να αποκτήσουν πρόσβαση σε κρίσιμα δεδομένα του οργανισμού. Ο έλεγχος παρείσδυσης αποτελεί μία προσομοίωση κυβερνοεπίθεσης με ελεγχόμενο τρόπο, που παρέχει πολύτιμες πληροφορίες σχετικά με την ύπαρξη ευπαθειών στα αγαθά του οργανισμού, την αποτελεσματικότητα των μέτρων προστασίας έναντι κακόβουλων ενεργειών, καθώς και το εύρος των επιπτώσεων (impact) που αυτές οι ενέργειες μπορούν να επιφέρουν. Επίσης, μπορούν να αναδείξουν αδυναμίες σε διαδικασίες, όπως

είναι εσφαλμένες ρυθμίσεις συστημάτων, καθώς και την ανάγκη για εκπαίδευση χρηστών.

Πώς – Πραγματοποιείτε, σε ετήσια βάση, ελέγχους παρείσδυσης στο δίκτυο, στα συστήματα και στις εφαρμογές σας. Διενεργήστε τους ελέγχους με αυστηρό και σαφές πεδίο εφαρμογής, λαμβάνοντας υπόψη το μέγεθος, την ωριμότητα και τις απαιτήσεις σας, καθώς και την κρισιμότητα των δεδομένων που επεξεργάζεστε. Υλοποιείστε διαδικασία έγκαιρης επιδιόρθωσης των εντοπισμένων ευπαθειών, δίνοντας προτεραιότητα στις σοβαρότερες, με βάση αναγνωρισμένα διεθνή πλαίσια μέτρησης κρισιμότητας ευπαθειών, όπως είναι το CVSS (Common Vulnerability Scoring System).