Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης

Από τη Θεωρία στην Πράξη:
Πώς το ΑΠΘ Εφαρμόζει τον Οδηγό 15 Σημείων της Εθνικής Αρχής για την Κυβερνοασφάλεια

Στο παρόν, παρουσιάζεται η περίπτωση του ΑΠΘ, εξειδικεύοντας μέσα από παραδείγματα εφαρμογής τον οδηγό 15 σημείων ενίσχυσης της κυβερνοασφάλειας για τα Πανεπιστημιακά Ιδρύματα που εξέδωσε η Εθνική Αρχή Κυβερνοασφάλειας. Για κάθε σημείο του οδηγού, παρατίθενται οι συστάσεις της ΕΑΚ και ακολουθεί η σύσταση υλοποίησης του ΑΠΘ, ενώ παρατίθενται και δύο επιπλέον σημεία ακόμα τα οποία κρίνουμε από την εμπειρία μας στο ΑΠΘ ότι είναι μεγάλης χρησιμότητας για τα ακαδημαϊκά ιδρύματα.

Σύνταξη κειμένου: Δρ. Γ. Πάλλας, ΜΨΔ ΑΠΘ
Επιμέλεια: Ν. Βασιλειάδης, Καθηγητής Τμ. Πληροφορικής ΑΠΘ, Πρόεδρος ΕΨΔ ΑΠΘ
Α. Αγορογιάννη, Προϊσταμένη ΜΨΔ ΑΠΘ

Νοέμβριος 2025

Περιεχόμενα

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.

Προτάσεις του ΑΠΘ

Στο ΑΠΘ, το σύνολο των δεδομένων, τόσο των υπηρεσιών του ιδρύματος, όσο και τα δεδομένα του IT Center που αφορούν όλες τις προσφερόμενες ψηφιακές υπηρεσίες, βρίσκεται αποθηκευμένο σε δύο συστήματα αποθήκευσης της NetApp που συγχρονίζονται live μεταξύ τους και τα οποία βρίσκονται σε δύο ξεχωριστά και φυσικώς απομακρυσμένα μεταξύ τους datacenters. Από αυτά τα συστήματα αποθήκευσης προσφέρονται οι κοινόχρηστοι αποθηκευτικοί χώροι τους οποίους έχουν διαθέσιμους όλες οι υπηρεσίες του ιδρύματος για την αποθήκευση των υπηρεσιακών τους δεδομένων, καθώς η πολιτική είναι ότι δεν πρέπει να παραμένουν αποθηκευμένα δεδομένα του ιδρύματος σε τοπικούς δίσκους υπολογιστών.

Τα προαναφερθέντα συστήματα αποθήκευσης έχουν εγγενώς δυνατότητα για snapshots, τα οποία γίνονται περιοδικά κάθε κάποιες ώρες και δίνουν την δυνατότητα σε υπαλλήλους και εργαζομένους να έχουν πρόσβαση σε στιγμιότυπα του παρελθόντος των δεδομένων τους, χωρίς να χρειάζεται παρέμβαση του IT Center. Με αυτόν τον τρόπο επιτυγχάνεται η προστασία των δεδομένων έναντι πλήθους απειλών: Ακούσια διαγραφή, τροποποίηση χωρίς πρόθεση ή και ransomware. Συγκεκριμένα για την τελευταία απειλή, δεδομένου του ότι οι χρήστες των

online αποθηκευτικών χώρων δεν έχουν δικαιώματα διαχειριστή σε αυτούς, πιθανή μόλυνση από ransomware ενός ή περισσοτέρων σταθμών εργασίας έχει ως αποτέλεσμα πολύ περιορισμένες απώλειες που περιορίζονται σε αποθηκευμένα δεδομένα λίγων ωρών στη χειρότερη περίπτωση, χωρίς να κινδυνεύουν τα ίδια τα snapshots.

Με την παραπάνω προτεινόμενη δομή αποθήκευσης, αντιμετωπίζονται και όλες οι περιπτώσεις όπου κάποιος εργαζόμενος λόγω λάθους προκαλέσει δυσλειτουργία σε κάποιο υποσύστημα, ή διαγραφή της συγκρότησης κάποιου συστήματος, ή ακόμα και διαγραφή κάποιου κρίσιμου λογισμικού που υποστηρίζει κάποια υπηρεσία. Η επαναφορά σε λειτουργικό αντίγραφο μπορεί να γίνει εντός λίγων λεπτών.

Στο ΑΠΘ, για την επιχειρησιακή συνέχεια του ιδρύματος, κρίσιμης σημασίας είναι η αυτοματοποιημένη λήψη αντιγράφων ασφαλείας τα οποία φυλάσσονται **offsite** και **offline** ώστε σε περίπτωση μεγάλης καταστροφής που καταστήσει μη-διαθέσιμο τον εξοπλισμό και τα δεδομένα σε όλα τα datacenter, να υπάρχει αντίγραφο από όπου να μπορεί να γίνει αποκατάσταση δεδομένων και υπηρεσιών. Η λήψη των αντιγράφων γίνεται σε μηνιαία βάση, η αποθήκευσή τους γίνεται σε φυλασσόμενο μέρος και γίνονται μηνιαίες δοκιμαστικές ανακτήσεις δεδομένων από τα αντίγραφα, πριν το μέσο αποθήκευσης σβηστεί για να περαστούν τα δεδομένα του επόμενου μήνα. Περισσότερες λεπτομέρειες για άλλες παραμέτρους της επιχειρησιακής συνέχειας παρατίθενται στο σημείο 17.

Πιο συγκεκριμένα, τα αντίγραφα ασφαλείας δημιουργούνται μηνιαίως σε LTO tape library και ακολουθείται στη συνέχεια η εξής διαδικασία: τα tapes φυλάσσονται offsite, ενώ υπάρχει ένα δεύτερο σετ tapes στα οποία γράφεται το backup του επόμενου μήνα, το σετ φυλάσσεται offsite, επιστρέφει στο datacenter το προηγούμενο set, γίνεται δοκιμαστική ανάκτηση από αυτό, και στη συνέχεια το σετ αποθηκεύει τα δεδομένα του επόμενου μήνα. Με αυτόν τον κύκλο ζωής των εφεδρικών αντιγράφων, είναι βέβαιο ότι πάντα υπάρχει ένα λειτουργικό αντίγραφο των δεδομένων.

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.

Προτάσεις του ΑΠΘ

Στο ΑΠΘ διατηρείται ενημερωμένος κατάλογος όλων των κρίσιμων συστημάτων (servers, switches, firewalls, workstations). Για κάθε σύστημα καταγράφεται σε ένα πληροφοριακό σύστημα μια σειρά από στοιχεία: λειτουργία, υπεύθυνος διαχείρισης, σχετιζόμενα τιμολόγια, επίπεδο κρισιμότητας και πιθανές εξαρτήσεις. Ειδικότερα για τα workstations του ΑΠΘ, γίνεται χρήση του open source εργαλείου OCS Inventory, το οποίο με τη χρήση ενός agent στο κάθε PC, έχει την δυνατότητα να δημιουργεί αυτόματα ευρετήριο με όλα τα workstations καθώς και ποια λογισμικά είναι εγκατεστημένα στο καθένα, σε ποιες εκδόσεις βρίσκονται και με την συνεργασία ενός επιπλέον plugin 'CVE search', στο ευρετήριο προστίθεται και η πληροφορία ενδεχόμενων ευπαθειών που υπάρχουν σε εγκατεστημένα λογισμικά. Στο ΑΠΘ είναι υπό μελέτη ο πιθανός διαχωρισμός του Asset Inventory από τον έλεγχο ευπαθειών (CVE search) και η χρήση του Wazuh agent για τις τελευταίες.

Επίσης, για την διαρκή καταγραφή των κινήσεων συσκευών και πόρων στο δίκτυο, λειτουργεί σύστημα το οποίο είναι διαρκώς logged-in σε όλες τις δικτυακές συσκευές (Huawei, Cisco & Dell) και καταγράφει ARP & MAC tables, από τα οποία ενημερώνονται διαρκώς οι σχετικές databases. Το σύστημα αυτό έχει δοθεί στο παρελθόν στα ακαδημαϊκά ιδρύματα μέσω του έργου ΗΦΑΙΣΤΟΣ.

Επιπλέον, γίνεται χρήση του open source εργαλείου LibreNMS, στο οποίο είναι περασμένο το σύνολο των δικτυακών συσκευών και των IoT devices, προκειμένου να διατηρούνται στατιστικά, να γίνεται έλεγχος καλής λειτουργίας και να εντοπίζονται εγκαίρως δυσλειτουργίες μέσω του ενσωματωμένου alerting συστήματος.

Όλα τα παραπάνω assets, αποστέλλουν logs στη syslog υποδομή (syslog-ng / rsyslog) και επιλεγμένα logs στο OpenSearch, με αποτέλεσμα να είναι στη συνέχεια δυνατή η συσχέτιση ενεργειών με συγκεκριμένα αγαθά, η έγκαιρη αναγνώριση προβλημάτων, και η δυνατότητα πλήρους ιχνηλασιμότητας. Ο συνδυασμός asset inventory , logging και monitoring δημιουργεί έτσι έναν ενιαίο μηχανισμό ορατότητας.

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.

Προτάσεις του ΑΠΘ

Σε όσα πληροφοριακά συστήματα υπάρχει διαθέσιμη επιλογή για MFA, αυτή θα πρέπει να αξιοποιείται. Για web εφαρμογές, είναι αποδεκτό το επίπεδο ασφάλειας όπου το MFA δεν απαιτείται σε κάθε είσοδο στην εφαρμογή, εάν αυτή γίνεται από browser από τον οποίο έχει γίνει ήδη πρόσφατα login με χρήση MFA. Έτσι, η απαίτηση για MFA γίνεται όταν ο χρήστης επιχειρεί να εισέλθει στην web εφαρμογή από θέση εργασίας/browser που το σύστημα δεν έχει ξανασυναντήσει. Αυτή η επιλογή από άποψη ασφάλειας και ευχρηστίας είναι επιθυμητή, αρκεί να συνδυάζεται με θέσεις εργασίας όπου είναι ενεργοποιημένη η κρυπτογράφηση δίσκων. Σε διαφορετική περίπτωση, με boot CD/USB μπορεί κάποιος με πρόσβαση στο φυσικό σύστημα να κάνει χρήση των authentication cookies που βρίσκονται στο προφίλ του χρήστη. Στο ΑΠΘ, με αυτόν τον τρόπο διασφαλίζεται η πρόσβαση σε εφαρμογές όπως το JIRA και το Slack, αλλά για πληροφοριακά συστήματα με μεγαλύτερες απαιτήσεις ασφαλείας όπως το Φοιτητολόγιο, η απαίτηση για MFA είναι σε κάθε login.

Ως προς τον τύπο του MFA, αυτό μπορεί να είναι αποστολή SMS, ή μπορεί να γίνεται χρήση κάποιου authenticator app (στο ΑΠΘ χρησιμοποιείται ο Google Authenticator). Στην περίπτωση αποστολής MFA κωδικού σε email, θα πρέπει να προσεχθεί να μην παραβιάζεται η αρχή του MFA: Θα πρέπει να είναι διαφορετικός ο κωδικός πρόσβασης στο email όπου έρχεται ο MFA κωδικός από τον κωδικό πρόσβασης στην υπό εξέταση πλατφόρμα.

Θα πρέπει να σημειωθεί ότι στην ιδανική περίπτωση, όλα τα πληροφοριακά συστήματα είναι κάτω από μία ενιαία ομπρέλα authentication (SSO - Single Sign-On), οπότε η ενσωμάτωση MFA αρκεί να γίνει στην κεντρική πλατφόρμα του SSO.

Τέλος, για όσες περιπτώσεις δεν είναι δυνατή η εφαρμογή MFA, μια προσέγγιση που ελαττώνει το ρίσκο είναι η υποχρεωτική χρήση VPN για την πρόσβαση στον πόρο που επιθυμούμε να προστατεύσουμε. Και πάλι φυσικά θα πρέπει η πρόσβαση στο VPN να γίνεται με διαφορετικά credentials (π.χ. hardware token, certificate, SMS OTP) από ό,τι ο πόρος που προστατεύουμε.

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.

Προτάσεις του ΑΠΘ

Σε όλους τους Linux-based εξυπηρετητές του ΑΠΘ είναι ενεργοποιημένη η αυτόματη εγκατάσταση των security upgrades, έτσι ώστε για όποια ευπάθεια έχει υπάρξει patch, αυτό να εγκαθίσταται αυτόματα, χωρίς να χάνεται χρόνος που μπορεί να αποβεί κρίσιμος για την ασφάλεια των συστημάτων. Τα υπόλοιπα upgrades που δεν αφορούν στην ασφάλεια, γίνονται στον χρόνο που θα επιλέξουν οι διαχειριστές.

Στα Windows συστήματα, όπως αναφέρθηκε αναλυτικά σε προηγούμενη ενότητα, γίνεται χρήση του OCS Inventory, το οποίο με τη χρήση ενός agent στο κάθε PC, έχει την δυνατότητα

να δημιουργεί αυτόματα ευρετήριο με όλα τα workstations καθώς και ποια λογισμικά είναι εγκατεστημένα στο καθένα, σε ποιες εκδόσεις βρίσκονται και με την συνεργασία ενός επιπλέον plugin 'CVE search', στο ευρετήριο προστίθεται και η πληροφορία ενδεχόμενων ευπαθειών που υπάρχουν σε εγκατεστημένα λογισμικά. Στο ΑΠΘ είναι υπό μελέτη ο πιθανός διαχωρισμός του Asset Inventory από τον έλεγχο ευπαθειών (CVE search) και η χρήση του Wazuh agent για τις τελευταίες. Αφού βρεθεί όπως περιγράφηκε το σύνολο των υπό αναβάθμιση λογισμικών, η διαδικασία εκκινείται κι ολοκληρώνεται μέσω του Chocolatey package manager, με χρήση ιδιωτικού software repository του ΑΠΘ.

Τα Windows updates αφού εξεταστούν από την αρμόδια ομάδα του IT Center, εγκαθίστανται με τη χρήση ιδιωτικής υποδομής WSUS Server του ΑΠΘ, ώστε να μην γίνεται απευθείας επικοινωνία των workstations με τους servers της Microsoft, τόσο για λόγους firewalling, όσο και για την αποφυγή σπατάλης bandwidth.

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.

Προτάσεις του ΑΠΘ

Σε όλο το campus του ΑΠΘ, στα workstations υπάρχει εγκατεστημένο ESET antivirus με συνδρομή ώστε να ανιχνεύονται εγκαίρως στα endpoints οι απειλές (είναι γνωστό ότι οι περισσότερες παραβιάσεις ξεκινάνε από ακούσια συνήθως ανθρώπινη ενέργεια στο endpoint). Συγκεκριμένα, πρόκειται για ESET On-Prem server και license για ESET Endpoint Antivirus με εκδόσεις για desktops & servers. Σε workstations και servers εγκαθίσταται ο ESET Agent και στέλνει στον ESET On-Prem Server data και reports, ώστε επιπλέον των βασικών ρυθμίσεων και ενημερώσεων να είναι δυνατός ο καθορισμός policies (αντίστοιχα με τα windows Group Policy Objects - GPO) για τον μαζικό ορισμό ρυθμίσεων.

Επίσης, σύμφωνα με τις καλές διεθνείς πρακτικές, είναι απενεργοποιημένη σε όλα τα workstations η δυνατότητα χρήσης USB μέσων αποθήκευσης, καθώς στο παρελθόν είχε παρατηρηθεί ότι είναι πολύ συχνό το φαινόμενο της σύνδεσης στα workstations USB μέσων αποθήκευσης μολυσμένων με ιούς, θέτοντας έτσι σε κίνδυνο διαρροής κι απώλειας δεδομένων το ίδρυμα.

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.

Προτάσεις του ΑΠΘ

Στο ΑΠΘ διεξάγονται ετήσια σεμινάρια προς τους διοικητικούς υπαλλήλους και τα μέλη ΔΕΠ, στα οποία γίνεται εκπαίδευση πάνω σε θέματα ασφάλειας. Αυτή η πρακτική φαίνεται μέσα στα τελευταία χρόνια να παράγει ορατή βελτίωση, μειώνοντας τη συχνότητα των περιστατικών phising και ransomware. Επιπλέον είναι υπό προμήθεια το λογισμικό FortiPhish, με το οποίο ήδη δοκιμαστικά έχουν διεξαχθεί αξιολογήσεις του επιπέδου ετοιμότητας της κοινότητας του ΑΠΘ απέναντι σε απόπειρες phishing.

Επιπλέον, σε ειδικό email alias του ιδρύματος, τα μέλη της πανεπιστημιακής κοινότητας προωθούν ύποπτα email επί των οποίων επιθυμούν την γνωμοδότηση του IT Center και λαμβάνουν από το helpdesk οδηγίες χειρισμού τους.

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.

Προτάσεις του ΑΠΘ

Στο ΑΠΘ, το δίκτυο είναι χωρισμένο σε VLANs ανά λογική οντότητα του ιδρύματος. Κάθε Τμήμα διαθέτει δικό του VLAN, όπως και κάθε υπηρεσία. Επίσης, και εντός Τμημάτων, ειδικού ενδιαφέροντος οντότητες (π.χ. Γραμματείες και Νησίδες Υπολογιστών) έχουν δικό τους VLAN, με ελεγχόμενη πρόσβαση μέσω firewall, του οποίου η πολιτική είναι deny by default.

Επιπλέον εφαρμόζεται συνεχής παρακολούθηση της δικτυακής δραστηριότητας μέσω ελέγχου των NetFlow δεδομένων. Από τα ευρήματα, ενεργοποιείται αυτόματα μηχανισμός ο οποίος μπλοκάρει την προβληματική κίνηση. Ταυτόχρονα, είναι σε εξέλιξη διαγωνισμός για προμήθεια Next Generation Firewalls ώστε να μπορέσει να εφαρμοστεί και DPI για αναγνώριση ακόμα περισσότερων περιπτώσεων απειλών.

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.

Προτάσεις του ΑΠΘ

Στο ΑΠΘ, η διαχείριση της προνομιακής πρόσβασης (PAM) ακολουθεί την αρχή της απόδοσης του ελαχίστου αναγκαίου δικαιώματος πρόσβασης σε κάθε εργαζόμενο για κάθε εφαρμογή. Στο πλαίσιο αυτό υπάρχει σύστημα διαχείρισης χρηστών στο οποίο υποστηρίζεται Role-Based Access Control (RBAC) όπου ορίζονται ρόλοι με συγκεκριμένα δικαιώματα για συγκεκριμένες εργασίες και επιπλέον μπορούν να αποδίδονται αυτοί οι ρόλοι από τους διαχειριστές στους χρήστες των εφαρμογών.

Για τον σκοπό αυτό, είναι απαραίτητο καταρχάς να υπάρχει υποδομή κεντρικοποίησης της αυθεντικοποίησης των χρηστών, πάνω σε ένα ενιαίο σύστημα (SSO – Single Sign-On). Από την

εμπειρία του ΑΠΘ, σε ακαδημαϊκό περιβάλλον εξυπηρετεί η χρήση των πρωτοκόλλων OAuth 2.0 & OpenID Connect (OIDC), όπου το πρώτο υλοποιεί τον έλεγχο πρόσβασης (authorization) και το δεύτερο υλοποιεί τον έλεγχο ταυτότητας (authentication). Τα πρωτόκολλα αυτά υλοποιούνται ενδεικτικά από τις εφαρμογές Keycloak και WSO2 Identity Server τις οποίες χρησιμοποιεί και το ΑΠΘ ως IdP (Identity Provider) servers.

Εναλλακτικά, μπορεί να χρησιμοποιηθεί εάν αυτό εξυπηρετεί περισσότερο στις υπάρχουσες υποδομές του ιδρύματος και το πρωτόκολλο SAML 2.0, το οποίο εξυπηρετεί τόσο τον έλεγχο ταυτότητας των χρηστών όσο και τον έλεγχο πρόσβασης των χρηστών στις εφαρμογές και τους πόρους των πληροφοριακών συστημάτων. Η προτεινόμενη εφαρμογή που υλοποιεί το SAML 2.0 είναι η SimpleSAMLphp και εξυπηρετεί ως IdP (Identity Provider) server.

Μία ενδεικτική εφαρμογή στην οποία σε ακαδημαϊκό περιβάλλον έχει ιδιαίτερη σημασία η σωστή απονομή των ελάχιστων απαραίτητων δικαιωμάτων και προσβάσεων, είναι τα συστήματα E-Learning / eClass. Στο ΑΠΘ αλλά και σε άλλα ιδρύματα όπου χρησιμοποιείται το Moodle με ιδιαίτερη παραμετροποίηση για τις ανάγκες τους, ο ιδρυματικός λογαριασμός δίνει πρόσβαση στο σύστημα E-Learning μέσω αντίστοιχου τρόπου πιστοποίησης (έλεγχος ταυτότητας μέσω SAML) και ο μόνος ρόλος που ανατίθεται στον χρήστη είναι αυτός του «Authenticated user» και τα δικαιώματα στο σύστημα είναι εξαιρετικά περιορισμένα. Οι ρόλοι «Student» και «Teacher» που αφορούν την πλειονότητα των χρηστών ανατίθενται μέσω συγχρονισμών με τα υποσυστήματα των Γραμματειών σε ό,τι αφορά τα προγράμματα σπουδών του Πανεπιστημίου και από την Υπηρεσία Υποστήριξης Ηλεκτρονικών Μαθημάτων για τα εκτός προγραμμάτων σπουδών. Ο ρόλος «Teacher» προϋποθέτει ανάθεση διδασκαλίας και ο ρόλος «Student» δήλωση μαθημάτων. Ρόλοι με περισσότερα προνόμια ή σε μεγαλύτερο εύρος ανατίθενται σπάνια/επιλεκτικά κατόπιν αιτιολόγησης, από τους διαχειριστές, και πάντα γίνεται προσπάθεια να ανατεθούν στο μικρότερο δυνατό εύρος που εξυπηρετεί τη συγκεκριμένη ανάγκη (για παράδειγμα ανάθεση ρόλου «manager» σε μάθημα ή κατηγορία μαθημάτων αντί για όλο το σύστημα).

Επιπλέον, δεδομένης της κινητικότητας που υπάρχει σε υπαλλήλους, διδάσκοντες, εργαζομένους και φοιτητές στα ιδρύματα, για την διατήρηση των προσβάσεων σύμφωνα με την αρχή της απόδοσης του ελάχιστου δικαιώματος πρόσβασης για κάθε εργασία, απαιτείται περιοδικός έλεγχος και αναθεώρηση των δικαιωμάτων πρόσβασης (π.χ. ανά εξάμηνο ή μετά από αποχώρηση προσωπικού ή μετά από αλλαγή ρόλου). Ιδανικά, σε ένα περιβάλλον όπου όλα τα πληροφοριακά συστήματα είναι διασυνδεδεμένα, η αναθεώρηση των δικαιωμάτων πρόσβασης γίνεται αυτόματα, και εκκινείται μετά από κάθε αλλαγή κατάστασης κάποιου ατόμου σε κάποιο κεντρικό πληροφοριακό σύστημα.

Παρομοίως, κατά την αποχώρηση οποιουδήποτε ατόμου από το ίδρυμα, μετά την καταχώριση της νέας κατάστασης στο σύστημα αυθεντικοποίησης των χρηστών, ανακαλούνται αυτόματα οι προσβάσεις και τα tokens από όλα τα υποσυστήματα (αυτοματοποιημένο offboarding). Στις περιπτώσεις όπου υπάρχουν εξαιρέσεις μη-διασυνδεδεμένων συστημάτων (π.χ. Slack, JIRA), το

αυτοματοποιημένο μέρος της διαδικασίας περιλαμβάνει και το άνοιγμα δελτίων προς τις ομάδες που θα πρέπει να προβούν σε manual ενέργειες για την αφαίρεση των προσβάσεων από τα συστήματα αυτά.

Σε επίπεδο υποδομών (Virtual Machines, Hypervisors, Database servers, Domain Controllers, Active Directory, LDAP, κλπ.), γίνεται χρήση privileged access management (PAM) για λογαριασμούς διαχειριστών (π.χ. απομονωμένα admin credentials, session recording), ώστε οι ειδικού σκοπού προσβάσεις με αυξημένες δικαιοδοσίες να εκτίθενται μόνο στα ελάχιστα δυνατά άτομα, και η χρήση τους να γίνεται με δυνατότητα καταλογισμού – καταγραφή διαστήματος πρόσβασης, εντολές που δόθηκαν, κλπ.

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.

Προτάσεις του ΑΠΘ

Στο ΑΠΘ χρησιμοποιείται open source λογισμικό για την παροχή του email service προς τα μέλη της ακαδημαϊκής κοινότητας. Για το φιλτράρισμα των email χρησιμοποιείται FortiMail, το οποίο είναι μια ολοκληρωμένη πλατφόρμα ασφάλειας email που συνδυάζει προηγμένο antispam, antivirus/antimalware, sandboxing και URL filtering για την προστασία από phishing, BEC και στοχευμένες επιθέσεις. Προσφέρει Data Loss Prevention (DLP) και encryption για ασφαλή

διακίνηση ευαίσθητων δεδομένων, ενώ ενσωματώνει μηχανισμούς authentication όπως SPF, DKIM και DMARC για επαλήθευση αποστολέων και μείωση spoofing. Υποστηρίζει πλήρες archiving & journaling, granular policy management, και μπορεί να λειτουργήσει ως gateway ή ως internal mail security layer, με εύκολη ενσωμάτωση στο υπάρχον δίκτυο και κεντρική διαχείριση μέσω FortiOS/FortiAnalyzer.

Επιπλέον, όπως αναφέρθηκε σε προηγούμενη ενότητα, σε ειδικό email alias του ιδρύματος, τα μέλη της πανεπιστημιακής κοινότητας προωθούν ύποπτα email επί των οποίων επιθυμούν την γνωμοδότηση του IT Center και λαμβάνουν από το helpdesk οδηγίες χειρισμού τους.

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.

Προτάσεις του ΑΠΘ

Στο ΑΠΘ, όλα τα νέα συστήματα και υπηρεσίες ενσωματώνουν μηχανισμούς ασφαλείας από το στάδιο του σχεδιασμού (αρχή “Security by Design”). Για τον σκοπό αυτό χρησιμοποιείται η ακόλουθη checklist για την διασφάλιση της τήρησης των προβλέψεων ασφαλείας για κάθε νέο πληροφοριακό σύστημα.

1. Προκαταρκτικός Σχεδιασμός

☐ Έχει πραγματοποιηθεί ανάλυση απειλών (Threat Modeling) για τη νέα υπηρεσία ή σύστημα.

☐ Έχουν τεκμηριωθεί οι απαιτήσεις ασφάλειας μαζί με τις λειτουργικές προδιαγραφές (authentication, encryption, access control).

☐ Έχουν ληφθεί υπόψη οι κανονιστικές απαιτήσεις (GDPR, εθνική νομοθεσία, πολιτικές πανεπιστημίου).

2. Διαχείριση Πρόσβασης και Ταυτοποίησης

☐ Όλοι οι λογαριασμοί λειτουργούν με βάση την αρχή του ελάχιστου δικαιώματος (Least Privilege).

☐ Δεν υπάρχουν κοινόχρηστοι ή γενικοί διαχειριστικοί λογαριασμοί.

☐ Η πρόσβαση προστατεύεται με πολυπαραγοντική ταυτοποίηση (MFA) όπου είναι εφικτό.

☐ Τα credentials αποθηκεύονται με ασφάλεια σε κεντρικό secrets vault (π.χ. HashiCorp Vault).

3. Δικτυακή Απομόνωση & Ελεγχόμενη Επικοινωνία

☐ Το νέο σύστημα έχει τοποθετηθεί σε κατάλληλο VLAN ή DMZ με σαφώς ορισμένα firewall rules.

☐ Έχουν καταγραφεί και εγκριθεί όλες οι εξερχόμενες και εισερχόμενες συνδέσεις.

☐ Οι υπηρεσίες δικτύου (π.χ. SSH, SNMP, API ports) είναι περιορισμένες στις απολύτως απαραίτητες.

4. Ενημερώσεις & Hardening

☐ Το λειτουργικό σύστημα και το λογισμικό είναι ενημερωμένα (patched) κατά την εγκατάσταση.

☐ Έχουν ενεργοποιηθεί στο λειτουργικό σύστημα ρυθμίσεις για αυτόματη εγκατάσταση των security updates.

☐ Έχουν εφαρμοστεί CIS Benchmarks ή ισοδύναμα πρότυπα ασφαλών ρυθμίσεων.

☐ Έχουν απενεργοποιηθεί όλες οι μη απαραίτητες υπηρεσίες και λογαριασμοί.

☐ Έχουν οριστεί ισχυρές πολιτικές κωδικών και lockout.

5. Logging & Monitoring

☐ Το σύστημα είναι συνδεδεμένο με τον κεντρικό log server και το OpenSearch.

☐ Οι βασικές ενέργειες (authentication, configuration changes, access logs) καταγράφονται πλήρως.

☐ Έχει γίνει δοκιμή ανίχνευσης συμβάντων (alert test) πριν την έναρξη παραγωγικής λειτουργίας.

6. Αξιολόγηση Ασφάλειας πριν την Παραγωγή

☐ Έχει πραγματοποιηθεί security review ή penetration test.

☐ Έχουν τεκμηριωθεί τα ευρήματα και διορθωθεί τα κρίσιμα ζητήματα πριν την παραγωγή.

☐ Υπάρχει σαφής διαδικασία rollback σε περίπτωση αστοχίας.

7. Λειτουργική Συντήρηση και Lifecycle Management

☐ Υπάρχει τεκμηρίωση ασφαλείας του συστήματος (π.χ. network diagram, ACLs, credentials policy).

☐ Έχει οριστεί υπεύθυνος διαχείρισης και συντήρησης.

☐ Υπάρχει πλάνο τακτικών ενημερώσεων και αναθεώρησης ασφάλειας (τουλάχιστον ετησίως).

Στη συνέχεια, σχετικά με την υλοποίηση, στο ΑΠΘ κάθε υπηρεσία στήνεται σε ξεχωριστό VM ή cluster από VMs, με βάση την αρχή **Infrastructure as Code (IaC)** και τη χρήση αυτοματοποιήσεων όπως η Ansible. Έτσι, η κάθε αλλαγή σε διαμόρφωση μιας υπηρεσίας υλοποιείται πρώτα ως merge request σε GitLab repo, εγκρίνεται από δύο reviewers (4-eyes principle) και στη συνέχεια η αλλαγή γίνεται deploy στους εξυπηρετητές της υπηρεσίας. Με την παραπάνω δομή, μπορεί να στηθεί ένας νέος κόμβος της υπηρεσίας αυτοματοποιημένα εντός ελάχιστου χρόνου, χωρίς ανθρώπινη παρέμβαση, γεγονός που καθιστά ταχύτατη την ανάκαμψη μετά από κάποιο καταστροφικό συμβάν. Το άλλο όφελος από την παραπάνω δομή είναι ότι διασφαλίζεται η ορθή καταγραφή των ενεργειών που εκτελούνται από τους χειριστές των συστημάτων, τόσο για λόγους ιστορικότητας, όσο και για λόγους ασφάλειας.

Οι παραπάνω διαδικασίες εξασφαλίζουν ότι η μήτρα από την οποία διαμορφώνονται οι εξυπηρετητές των υπηρεσιών πληροί όλες τις προδιαγραφές ασφαλείας (μηχανισμοί updating, firewall, απενεργοποίηση περιττών services, κλπ.), και οι μηχανισμοί Infrastructure as Code (IaC) εξασφαλίζουν ότι ακόμα και αν γίνει από κάποιον administrator κάποια τοπική δοκιμαστική

αλλαγή και αυτή ξεχαστεί, οι αυτοματοποιημένες διαδικασίες μέσω Ansible και IaC, σύντομα θα την εξαλείψουν.

Ασφαλής Διαμόρφωση Διαμοιρασμού Δεδομένων

Ειδικότερα σχετικά με το ransomware, κομβικής σημασίας είναι η οργάνωση των δεδομένων, η αποθήκευσή τους και ο τρόπος διαμοιρασμού τους μεταξύ των εργαζομένων. Στο ΑΠΘ, προκειμένου να μπορεί να επιτελεστεί το διοικητικό και ερευνητικό έργο με ασφάλεια και ταχύτητα, έχει αναπτυχθεί μια υποδομή ανταλλαγής και αποθήκευσης αρχείων σε ένα κοινόχρηστο δικτυακό αποθηκευτικό χώρο, διευκολύνοντας την συνεργασία διοικητικών υπηρεσιών και ερευνητικών ομάδων του ΑΠΘ. Η υποδομή κάνει χρήση των κεντρικών Windows Domain Controllers οι οποίοι διαμοιράζουν αποθηκευτικό χώρο της αποθηκευτικής συστοιχίας της NetApp σύμφωνα με τις ανάγκες των χρηστών και των υπηρεσιών.

Με τον τρόπο αυτό, αποφεύγεται το φαινόμενο της ανταλλαγής email με συνημμένα μεταξύ χρηστών, καθώς και της μεταφοράς αρχείων μέσω υπηρεσιών τρίτων (π.χ. WeTransfer) οι οποίες εκθέτουν σε κίνδυνο διαρροής και επεξεργασίας άνευ συναίνεσης τα υπηρεσιακά δεδομένα. Επιπλέον, λόγω της προσωποποιημένης πρόσβασης στους κοινόχρηστους φακέλους, τα δεδομένα είναι διαθέσιμα μόνο στα απολύτως απαραίτητα άτομα, καθιστώντας δυνατό τον έλεγχο πρόσβασης αναλόγως της διαβάθμισης των πληροφοριών.

Σε περισσότερη λεπτομέρεια, η υπηρεσία παρέχεται στη διεύθυνση \\<central server>\Groups και είναι προσβάσιμη μέσω του πρωτοκόλλου SMB εντός δικτύου ΑΠΘ (on-campus ή μέσω VPN). Η υπηρεσία χρησιμοποιεί αποθηκευτικό χώρο (κεντρικό SMB share) που παρέχεται απευθείας από την κεντρική υποδομή storage της NetApp, η οποία χρησιμοποιεί το Active Directory των κεντρικών Domain Controllers για το authentication & authorization των χρηστών. Συγκεκριμένα, έχει δημιουργηθεί στο NetApp ένα SVM (Storage Virtual Machine) το οποίο έχει γίνει join στο κεντρικό windows domain του ΑΠΘ.

Η δημιουργία και η διαχείριση των φακέλων εντός του share (όνομα, διαθέσιμος χώρος) γίνεται μέσω των ansible modules που παρέχει η NetApp. Η πρόσβαση των χρηστών σε κάθε φάκελο ορίζεται μέσω των NTFS δικαιωμάτων που αποδίδονται από τους Domain Controllers. Για την αυτόματη απόδοση των NTFS δικαιωμάτων χρησιμοποιείται ένα αρχείο json όπου αποθηκεύονται τα δικαιώματα ανά φάκελο και ένα script που εκτελείται μέσω GitLab CI/CD. Ειδικά για τα managed PCs έχει ρυθμιστεί μέσω DFS το path \\<server name>\dfs\files\ (που δείχνει στον ίδιο χώρο) και ρυθμίζεται μέσω Group Policy ως mapped drive ώστε να το βρίσκει ο χρήστης αυτόματα στο "This PC".

Με την παραπάνω δομή, είναι διαθέσιμο και το χαρακτηριστικό ιδιωτικότητας του Access Based Enumeration, όπου σε κάθε χρήστη είναι ορατοί μόνο οι φάκελοι στους οποίους του έχει δοθεί πρόσβαση, δηλαδή στο \\<central server>\Groups που περιέχει όλους τους φακέλους που έχουν δημιουργηθεί για όλες τις υπηρεσίες και τους σκοπούς, ο χρήστης βλέπει μόνο αυτούς που τον αφορούν.

Σημειώνεται, ότι με την παραπάνω δομή, εκτός της τήρησης της εμπιστευτικότητας και της ελεγχόμενης πρόσβασης στις πληροφορίες σύμφωνα με τη διαβάθμισή τους, οι χρήστες και ερευνητές απολαμβάνουν επιπλέον και τα ακόλουθα χαρακτηριστικά:

- τακτική λήψη αντιγράφων ασφαλείας και διατήρησή τους για 60 ημέρες
- εύκολη (χωρίς εμπλοκή διαχειριστή) επαναφορά διαγραμμένων αρχείων από αντίγραφα ασφαλείας και ανάκτηση προηγούμενων εκδόσεων των αρχείων
- ασφάλεια στη μεταφορά δεδομένων και υψηλές ταχύτητες μεταφοράς εντός του δικτύου δεδομένων του ΑΠΘ
- προστασία των αρχείων από τους κινδύνους που διατρέχουν όταν είναι αποθηκευμένα τοπικά στον υπολογιστή (ιοί, ransomware, βλάβες υλικού)

Προκειμένου να είναι δυνατές οι προβλέψεις αυτής της ενότητας, εξυπηρετεί να είναι οι θέσεις εργασίας (workstations) όλων των εργαζομένων υπό την κεντρική διαχείριση του IT Center. Για να επιτευχθεί αυτό, θα πρέπει να υπάρχουν τα κατάλληλα εργαλεία και διαδικασίες για εξ αποστάσεως διαχείριση του συνόλου των Η/Υ και για κεντρική εγκατάσταση και παραμετροποίηση του λειτουργικού και των εγκατεστημένων λογισμικών. Ακολουθούν ορισμένες συστάσεις και πρακτικές που στην περίπτωση του ΑΠΘ έχουν φανεί χρήσιμες για τη διαχείριση των περίπου 2190 workstations των εργαζομένων του.

Αρχικά, για να μπορούν να γίνουν γρήγορα image deployments για το αρχικό στήσιμο των υπολογιστών χρησιμοποιείται ένας FOG server (https://fogproject.org/) στον οποίο είναι καταχωρημένοι ανά groups όλοι οι Η/Υ και έχουν γίνει upload τα «golden images» τα οποία γίνονται deploy. Τα «golden images» δημιουργούνται σε VM με τις ελάχιστες δυνατές παρεμβάσεις ώστε το σύνολο των ρυθμίσεων και των πολιτικών να εφαρμόζεται κεντρικά. Στο BIOS, μεταξύ άλλων, έχουν γίνει ρυθμίσεις για ενεργοποίηση του wake on LAN και έχει ρυθμιστεί το boot order ώστε ως 1η συσκευή να είναι η κάρτα δικτύου και ως 2η ο δίσκος.

Στη συνέχεια, κατά το image deployment, κατά την εκκίνηση των υπολογιστών γίνεται PXE boot, λαμβάνουν IP μέσω static DHCP και γίνεται έλεγχος αν έχει δοθεί κάποιο task από τον FOG server, το οποίο συνήθως είναι το να γίνει το image deployment. Αφότου ολοκληρωθεί η διαδικασία, ο FOG server μέσω του FOG client κάνει join το workstation στο domain και στη συνέχεια πάλι μέσω του FOG client δίνεται η δυνατότητα να σταλούν σε ομάδες Η/Υ μαζικά snapins, δηλαδή διάφοροι αυτοματισμοί (π.χ. με PowerShell scripts).

Τέλος, μετά την πρώτη επανεκκίνηση, μέσω της on-premises open source υποδομής Chocolatey γίνεται deployment των επιθυμητών λογισμικών ανάλογα με το αν ο Η/Υ ανήκει σε διοικητικό υπάλληλο ή βρίσκεται σε κοινόχρηστο εργαστήριο φοιτητών. Εφαρμόζονται τα αντίστοιχα group policies objects από το Active Directory και ο Η/Υ είναι πλέον έτοιμος προς χρήση.

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.

Προτάσεις του ΑΠΘ

Στο ΑΠΘ υπάρχει κεντρική syslog υποδομή (υλοποιημένη με syslog-ng και μελλοντικά με rsyslog) στην οποία στέλνονται logs από όλα τα Linux VMs. Εκεί τα logs διατηρούνται για ένα χρόνο, εξασφαλίζοντας τη δυνατότητα πλήρους ιχνηλασιμότητας σε βάθος χρόνου και καθιστώντας την διερεύνηση περιστατικών γρήγορη και αποδοτική. Επιπλέον, συγκεκριμένες κατηγορίες logs στέλνονται σε υποδομή OpenSearch. Εκεί τα logs επεξεργάζονται και αποθηκεύονται σε δομημένη και αναζητήσιμη μορφή, ενώ υπάρχουν και ειδικά dashboards για οπτικοποίηση.

Κάποιες υπηρεσίες όπως το DHCP, το VPN (EduVPN) και η υποδομή ασύρματου δικτύου (υλοποιημένη με Huawei AirEngine 9700M1) κάνουν επιπλέον logging μέσω Radius σε database servers (υλοποιημένοι με Percona server 5.7 και 8) ενισχύοντας τη δυνατότητα ταυτοποίησης χρηστών και συσκευών.

Για ειδικές περιπτώσεις, όπως η router & switching υποδομή, υπάρχουν ειδικά διαμορφωμένα scripts που φιλτράρουν το logging της υποδομής και εμφανίζουν μόνο τα αξιόλογα ευρήματα. Ταυτόχρονα η router & switching υποδομή καταγράφει σε πραγματικό χρόνο όλες τις συσκευές που κινούνται στο δίκτυο.

Τέλος, σε όλους τους εξυπηρετητές και τις δικτυακές συσκευές είναι κεντρικά ρυθμισμένος ο NTP server του ιδρύματος, ώστε τα ρολόγια όλων των υπηρεσιών να είναι συγχρονισμένα, ώστε να μπορούν να αξιοποιηθούν τα logs τους σε περιπτώσεις διερεύνησης συμβάντων.

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.

Προτάσεις του ΑΠΘ

Το ΑΠΘ διαθέτει Μηχανισμό Διαχείρισης Περιστατικών Ψηφιακής Ασφάλειας που προβλέπει:

- Άμεση αναφορά περιστατικών
- Τεκμηρίωση και διερεύνηση περιστατικών
- Ανάκτηση και αποκατάσταση υπηρεσιών
- Αναθεώρηση πρακτικών/διαδικασιών και πρόληψη μελλοντικών απειλών

Οι χρήστες στην αντίληψη των οποίων έρχεται κάποιο συμβάν που σχετίζεται με την ασφάλεια πληροφοριών, ή κάποια ασυνήθιστη συμπεριφορά κάποιου πληροφοριακού συστήματος, οφείλουν να το αναφέρουν το ταχύτερο δυνατόν στη Μονάδα Ψηφιακής Διακυβέρνησης. Μία τεκμηριωμένη διαδικασία διαχείρισης περιστατικών που σχετίζονται με την ασφάλεια είναι κρίσιμη προκειμένου το ίδρυμα να μπορεί στον ελάχιστο δυνατό χρόνο να ανιχνεύσει περιστατικά ασφάλειας σε εξέλιξη, να περιορίσει τις συνέπειες, να αναγνωρίσει τι ακριβώς συνέβη και να οχυρωθεί απέναντι σε παρόμοιες απειλές στο μέλλον.

Για τον σκοπό αυτό, σύμφωνα και με τις διεθνείς πρακτικές, όταν διαπιστώνεται ένα περιστατικό ασφάλειας, αρχικά ενημερώνεται η IR ομάδα (μέσω Viber & Slack) στην οποία συμμετέχουν όλοι οι προϊστάμενοι των τμημάτων του IT Center προκειμένου να συντονιστεί η δράση των ομάδων και στη συνέχεια συμπληρώνεται από τους εμπλεκόμενους η παρακάτω αναφορά, ώστε να διασφαλιστεί ότι ακολουθήθηκαν όλες οι καθορισμένες διαδικασίες.

ΔΕΛΤΙΟ ΑΝΑΦΟΡΑΣ ΠΕΡΙΣΤΑΤΙΚΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Συνοπτική περιγραφή περιστατικού:

…

Κρισιμότητα περιστατικού (1-10):

Αναλυτικά στοιχεία περιστατικού:

1. Στοιχεία ατόμου που αναφέρει το περιστατικό

…

2. Ημερομηνία και ώρα εκδήλωσης του περιστατικού

…

3. Ημερομηνία και ώρα που αναφέρθηκε το περιστατικό στο Πανεπιστήμιο

…

4. Αναλυτική περιγραφή του περιστατικού

…

5. Πληροφοριακά Συστήματα ή φυσικός χώρος ή άτομα στα οποία εκδηλώθηκε το περιστατικό

…

6. Τυχόν μάρτυρες του περιστατικού

…

7. Εκτιμώμενη αιτία εκδήλωσης του περιστατικού

…

8. Συνέπειες και επίπεδο κρισιμότητας του περιστατικού

…

9. Συλλεχθέντα στοιχεία για τη διερεύνηση του περιστατικού

…

10. Ενημέρωση για την ενδεχόμενη εμφάνιση του περιστατικού περισσότερες φορές

…

11. Χρόνος επίλυσης του προβλήματος

…

12. Διορθωτικά μέτρα και σχετικό χρονοδιάγραμμα

…

13. Ενημέρωση θιγόμενων χρηστών ή άλλων ατόμων που επηρεάστηκαν από το περιστατικό και γνωστοποίηση στις αρμόδιες αρχές σύμφωνα με την κείμενη νομοθεσία

…

14. Ενδεχόμενες συστάσεις σε θιγόμενους χρήστες ή άλλα άτομα που επηρεάστηκαν από το περιστατικό, με σκοπό τον μετριασμό των αρνητικών επιπτώσεών του

…

Τέλος, σχετικά με ενδεχόμενη αναφορά του συμβάντος στην Εθνική Αρχή Κυβερνοασφάλειας: Αυτή τη στιγμή, σύμφωνα με το ισχύον κανονιστικό πλαίσιο, η αναφορά των συμβάντων ασφαλείας είναι υποχρεωτική κατά NIS2 για ΦΕΒΥ (Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών – τράπεζες, παρόχους ενέργειας, κλπ.), και ΠΨΥ (Παρόχους Ψηφιακών Υπηρεσιών) και εθελοντική για όλους τους λοιπούς. Καθώς τα ακαδημαϊκά ιδρύματα δεν εμπίπτουν στην οδηγία NIS2, είναι στη διακριτική τους ευχέρεια το αν θα υποβάλουν την αναφορά στην ΕΑΚ. Η γνώμη του ΑΠΘ είναι ότι κυβερνοεπιθέσεις και συμβάντα ασφαλείας τα οποία δεν φαίνεται να είναι μεμονωμένες περιπτώσεις και ίσως αποτελούν μέρος ενός ευρύτερου συμβάντος ή φαίνεται να αφορούν πολύ μεγάλο εύρος συστημάτων εντός του ιδρύματος, καλό θα ήταν να αναφερθούν στην ΕΑΚ για έγκαιρη πρόληψη σε εθνικό επίπεδο.

Εάν το περιστατικό κυβερνοασφάλειας αφορά υποκλοπή στοιχείων και δεδομένων χρηστών, το ίδρυμα απενεργοποιεί τους επίμαχους λογαριασμούς και ειδοποιεί τους χρήστες τους για το συμβάν, σύμφωνα και με τα προβλεπόμενα στον Γενικό Κανονισμό για την Προστασία των Δεδομένων (ΓΚΠΔ – GDPR). Στην περίπτωση που η διαρροή δεδομένων αφορά μεγάλη ομάδα χρηστών, το IT Center του ιδρύματος ενδέχεται κατά περίπτωση να απενεργοποιήσει προσωρινά την υπηρεσία μέχρι να βρεθεί το πρόβλημα από το οποίο προήλθε η διαρροή, ώστε να γίνει δυνατή η επιδιόρθωση χωρίς να υπάρξει περαιτέρω διαρροή. Ταυτόχρονα προβλέπεται ενημέρωση και προς τους χρήστες, των οποίων τα δεδομένα εκτέθηκαν, καθώς και το σε τι ακριβώς δεδομένα αφορά η έκθεση αυτή, κατά τις προβλέψεις του νόμου.

ΠΡΟΛΗΨΗ

Προκειμένου να ελαχιστοποιηθεί το πλήθος των περιστατικών τα οποία σχετίζονται με την ασφάλεια ή/και την επιχειρησιακή συνέχεια του ιδρύματος, στον τομέα της πρόληψης, το ΑΠΘ συστηματικά αξιολογεί τους κινδύνους στους οποίους είναι εκτεθειμένα τα δεδομένα και οι υπηρεσίες του προκειμένου να καταρτίσει πλάνα αντιμετώπισης κι ανάκαμψης.

Για τον σκοπό αυτό εκτελούνται περιοδικά οι παρακάτω διεργασίες:

- Καταγραφή και κατηγοριοποίηση περιουσιακών στοιχείων (Asset Inventory)
  (όπως αναλύθηκε στην ενότητα «Καταγραφή Υλικού και Λογισμικού»)

- Αναγνώριση απειλών (Threat Identification)

  (με χρήση NetFlow processing, όπως αναλύθηκε στην ενότητα «Κατακερματισμός Δικτύου», και με endpoint protection με χρήση ESET antivirus όπως αναλύθηκε στην ενότητα «Ανίχνευση και Ανταπόκριση σε Σημεία Τερματικών (EDR)»)

- Εκτίμηση ευπαθειών (Vulnerability Assessment)

Διενεργούνται τουλάχιστον ετήσιοι έλεγχοι ευπαθειών (με εργαλεία όπως Nessus, OpenVAS κ.α.), όλων των υπηρεσιών και εξυπηρετητών που είναι εκτεθειμένοι στο internet, αλλά και των εσωτερικών συστημάτων. Τα αποτελέσματα τεκμηριώνονται και ταξινομούνται βάσει σοβαρότητας (CVSS) και πιθανών επιπτώσεων στις υπηρεσίες, και ακολουθεί η αντιμετώπιση των ευρημάτων. Επίσης διενεργούνται έλεγχοι για την διαπίστωση περιπτώσεων χρηστών με passwords τα οποία δεν πληρούν τις απαιτήσεις ασφαλείας.

- Ανάλυση επιπτώσεων (Impact Analysis)

  Για κάθε κίνδυνο που θα εντοπιστεί, εκτιμάται η επίπτωση στη διαθεσιμότητα, ακεραιότητα και εμπιστευτικότητα των υπηρεσιών, προτεραιοποιούνται οι κίνδυνοι που επηρεάζουν κρίσιμες λειτουργίες (π.χ. authentication, DNS, core routing) και ακολουθούν οι ενέργειες εξάλειψης του κινδύνου.

- Μέτρα αντιμετώπισης (Risk Mitigation)

  Καθορίζονται διορθωτικά μέτρα (firmware patching, OS upgrade, libraries upgrade, network segmentation, access control, redundancy). Για κάθε μέτρο ορίζεται υπεύθυνος, χρονοδιάγραμμα και τρόπος επαλήθευσης.

- Περιοδική επανεκτίμηση κινδύνων

  Η αξιολόγηση κινδύνων επαναλαμβάνεται σε τακτική βάση (κατ' ελάχιστον μία φορά το έτος) ή μετά από σημαντικές αλλαγές υποδομών. Επιπλέον, κρατείται ιστορικό αρχείο με όλες τις εκτιμήσεις και ενέργειες που ελήφθησαν.

- Διασύνδεση με Αντιμετώπιση Περιστατικών

  Από τα αποτελέσματα της αξιολόγησης κι αντιμετώπισης κινδύνων ενδέχεται να χρειαστεί να ενημερωθεί η Πολιτική Διαχείρισης Περιστατικών Ασφάλειας, εάν η αντιμετώπιση των ευρημάτων δεν καλύπτεται από την υπάρχουσα πολιτική.

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.

Προτάσεις του ΑΠΘ

Σε προηγούμενη ενότητα παρουσιάστηκε αναλυτικά η πρακτική της κεντρικής διαχείρισης των θέσεων εργασίας του ΑΠΘ. Με την πρακτική αυτή, επιτυγχάνεται κι ένας επιπλέον στόχος, ο περιορισμός ανεξέλεγκτης χρήσης λογισμικού. Η ανεξέλεγκτη χρήση λογισμικού στις θέσεις εργασίας κατά την διακριτική ευχέρεια των υπαλλήλων και του προσωπικού, οδηγεί συχνά τόσο στην εγκατάσταση malware στους υπολογιστές, όσο και λογισμικού μη αδειοδοτημένης χρήσης, το οποίο όπως έχει συμβεί στο παρελθόν μπορεί να επιφέρει νομικές συνέπειες και πρόστιμα στα ιδρύματα. Με την καθολική εφαρμογή της κεντρικής διαχείρισης υπάρχει άμεσος έλεγχος ως προς τα εγκατεστημένα λογισμικά ώστε να προλαμβάνονται δυσάρεστες καταστάσεις.

14. Παρακολούθηση για Crypto Mining, Tor και Υπηρεσίες Torrent

Γιατί – Η μη εξουσιοδοτημένη εξόρυξη κρυπτονομισμάτων και η μη κατάλληλη χρήση υπηρεσιών Tor και Torrent 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 τα δεδομένα του ιδρύματος, 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.

Προτάσεις του ΑΠΘ

Όπως αναλύθηκε προηγουμένως στην ενότητα «Κατακερματισμός Δικτύου», στο ΑΠΘ γίνεται από αυτοματοποιημένο μηχανισμό διαρκής έλεγχος των ροών NetFlow και ακολούθως περιορίζονται αυτόματα τυχόν απειλές που ανιχνεύονται (DoS attacks, virus port scanning, excessive flows), ενώ γίνεται και το αντίστοιχο reporting. Ως συνέπεια, περιπτώσεις κακόβουλης ή υπέρμετρης χρήσης των δικτυακών πόρων γίνεται εγκαίρως αντιληπτή και σε αρκετές περιπτώσεις περιορίζεται αυτόματα, προτού αποτελέσει κίνδυνο για την ασφάλεια.

Επίσης, όπως αναλύθηκε στην ενότητα «Καταγραφή Υλικού και Λογισμικού», επειδή σε όλες τις διοικητικές θέσεις εργασίας υπάρχει εγκατεστημένος ο OCS Inventory agent, τυχόν ακατάλληλα λογισμικά ανιχνεύονται και ακολουθεί η απεγκατάστασή τους και οι κατάλληλες συστάσεις στους χρήστες. Επιπλέον, λόγω του κεντρικά εγκατεστημένου ESET antivirus, τα λογισμικά που

αποτελούν άμεσο κίνδυνο δεν είναι δυνατόν να εγκατασταθούν εξαρχής, γιατί με την ολοκλήρωση του downloading υφίστανται περιορισμό καραντίνας από το antivirus.

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).

Προτάσεις του ΑΠΘ

Στο ΑΠΘ διενεργούνται τουλάχιστον ετήσιοι έλεγχοι ευπαθειών (με εργαλεία όπως Nessus, OpenVAS και αντίστοιχα), όλων των υπηρεσιών και εξυπηρετητών που είναι εκτεθειμένοι στο internet, αλλά και των εσωτερικών συστημάτων. Τα αποτελέσματα τεκμηριώνονται και ταξινομούνται βάσει σοβαρότητας (CVSS) και πιθανών επιπτώσεων στις υπηρεσίες, και

ακολουθεί η αντιμετώπιση των ευρημάτων. Επίσης διενεργούνται έλεγχοι για την διαπίστωση περιπτώσεων χρηστών με passwords τα οποία δεν πληρούν τις απαιτήσεις ασφαλείας.

Σχετικά με την προστασία από επιθέσεις που έχουν σκοπό να υποκλέψουν στοιχεία και δεδομένα χρηστών, αυτές καταρχάς αντιμετωπίζονται με το να διασφαλιστεί ότι οι χρήστες και οι διαχειριστές υπηρεσιών του ιδρύματος χρησιμοποιούν MFA όπου είναι δυνατόν, και έχουν ασφαλείς κωδικούς. Στο πλαίσιο αυτό είναι πάγια στρατηγική του ιδρύματος να ελέγχονται οι κωδικοί των χρηστών και διαχειριστών για την επαρκή ασφάλειά τους και, σε περίπτωση που βρίσκονται ανεπαρκείς κωδικοί, οι κάτοχοι υποχρεώνονται σε αλλαγή του κωδικού τους. Ταυτόχρονα, υπάρχουν μηχανισμοί οι οποίοι σε περιπτώσεις επανειλημμένων αποτυχημένων εισαγωγών κωδικού, απενεργοποιούν την πρόσβαση ή ενεργοποιούν χρονοκαθυστέρηση, ώστε να μην γίνει δυνατό να βρεθεί ο κωδικός με μεγάλο πλήθος δοκιμών (brute force).

16. Προστασία προσωπικών δεδομένων

Πέρα από τα παραπάνω 15 σημεία του οδηγού για την κυβερνοασφάλεια των ακαδημαϊκών ιδρυμάτων, το ΑΠΘ επιθυμεί να προσθέσει και δύο σημεία ακόμα, χρήσιμα για την περαιτέρω οχύρωση έναντι κυβερνοαπειλών και λοιπών καταστροφικών συμβάντων.

Από τη φύση του αντικειμένου τους τα ακαδημαϊκά ιδρύματα φιλοξενούν στις υποδομές των πληροφοριακών τους συστημάτων δεδομένα προσώπων τα οποία υπάγονται στις σχετικές εθνικές νομοθεσίες, ενώ κάποιο υποσύνολο αυτών υπάγεται και στον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR). Παρακάτω δίνονται κάποιες καλές πρακτικές για τον σωστό χειρισμό των δεδομένων και την κατά το δυνατό ελάχιστη έκθεσή τους σε κινδύνους. Οι καλές πρακτικές αφορούν τόσο στα δεδομένα που αποθηκεύονται στα πληροφοριακά συστήματα και αφορούν τους χρήστες, όσο και στα ψηφιακά ίχνη που αφήνει η χρήση των υπηρεσιών εκ μέρους των χρηστών.

- Ελαχιστοποίηση δεδομένων (Data Minimization)

  Καταγράφονται μόνο τα απολύτως απαραίτητα δεδομένα για σκοπούς ασφάλειας και λειτουργίας και αποφεύγεται η καταγραφή περιττών προσωπικών δεδομένων χρηστών.

- Ανωνυμοποίηση και ψευδωνυμοποίηση (Anonymization / Pseudonymization)

Όπου είναι εφικτό, προσωπικά αναγνωρίσιμα στοιχεία (όπως usernames ή IPs) ψευδωνυμοποιούνται πριν την αποθήκευση. Επίσης, τα αναγνωριστικά χρηστών αποσυνδέονται από τα τεχνικά δεδομένα πρόσβασης όταν δεν απαιτείται ταυτοποίηση.

- Περιορισμένη πρόσβαση στα δεδομένα

  Εφαρμόζονται ρόλοι πρόσβασης (RBAC) και αρχή του ελάχιστου δικαιώματος (Least Privilege), όπως αναλύθηκαν παραπάνω. Οι διαχειριστές έχουν πρόσβαση μόνο σε εκείνα τα δεδομένα που σχετίζονται με τις αρμοδιότητές τους.

- Κρυπτογράφηση

  Όλα τα δεδομένα πρέπει να μετακινούνται πάνω στο δίκτυο κρυπτογραφημένα με σύγχρονα πρωτόκολλα κρυπτογράφησης (encryption in transit). Η δε αποθήκευση των δεδομένων πρέπει να γίνεται κατά το δυνατόν σε κρυπτογραφημένα volumes ή databases (encryption at rest). Τα ευαίσθητα προσωπικά δεδομένα των χρηστών (κωδικοί πρόσβασης) πρέπει να αποθηκεύονται κρυπτογραφημένα ή hashed.

- Καθορισμένη πολιτική διατήρησης (Retention Policy)

  Τα δεδομένα των χρηστών διατηρούνται για το διάστημα που προβλέπεται στη νομοθεσία και εξειδικεύεται στην πολιτική διατήρησης δεδομένων, και μετά διαγράφονται αυτόματα. Η πολιτική τεκμηριώνεται και ελέγχεται τακτικά.

- Καταγραφή πρόσβασης στα δεδομένα (Audit Trails)

  Καταγράφεται κάθε πρόσβαση, ανάγνωση ή τροποποίηση των logs, ώστε να υπάρχει πλήρης ιχνηλασιμότητα. Οι έλεγχοι αυτοί δεν πρέπει να περιλαμβάνουν προσωπικά δεδομένα χρηστών πέραν των απολύτως αναγκαίων.

- Ενημέρωση και εκπαίδευση προσωπικού

  Γίνονται συστηματικές εκπαιδεύσεις του προσωπικού και των μελών ΔΕΠ πάνω σε θέματα κυβερνοασφάλειας, αλλά και χρήσης των διαθέσιμων υπηρεσιών του ιδρύματος, προκειμένου η εξυπηρέτηση της πανεπιστημιακής κοινότητας να γίνεται κατά το δυνατόν μέσα από τις υποδομές του ιδρύματος και όχι μέσω ανεξέλεγκτων υπηρεσιών τρίτων.

  Αξίζει να σημειωθεί ότι σύμφωνα με το ισχύον κανονιστικό πλαίσιο του ΓΚΠΔ περί

Υπευθύνων Επεξεργασίας, δεν είναι αποδεκτό να γίνεται αποθήκευση ή/και επεξεργασία προσωπικών δεδομένων (π.χ. φοιτητών) μέσα από online εργαλεία που χρησιμοποιούνται από το προσωπικό/μέλη ΔΕΠ με χρήση προσωπικών λογαριασμών.

Ειδικά για το προσωπικό του IT Center, θα πρέπει κατά την ανάληψη καθηκόντων να υπογράφει δήλωση εχεμύθειας ώστε να υπάρχει νομική κάλυψη του ιδρύματος έναντι διαρροών οποιουδήποτε είδους.

17. Φυσική, Λειτουργική Ασφάλεια & Επιχειρησιακή Συνέχεια

Στο σύγχρονο περιβάλλον των ακαδημαϊκών ιδρυμάτων, όπου η εκπαίδευση, η έρευνα και η τεχνολογική καινοτομία εξαρτώνται απόλυτα από τη συνεχή και απρόσκοπτη λειτουργία κρίσιμων υποδομών, η διασφάλιση της φυσικής και λειτουργικής ασφάλειας αποκτά καθοριστική σημασία. Η προστασία ανθρώπινου δυναμικού, εγκαταστάσεων, εξοπλισμού, δεδομένων και τεχνογνωσίας δεν αποτελεί μόνο τεχνική ή διοικητική υποχρέωση, αλλά θεμέλιο για την αξιοπιστία και τη βιωσιμότητα του ιδρύματος.

Παράλληλα, οι απειλές, από φυσικές καταστροφές και τεχνολογικές βλάβες έως κυβερνοεπιθέσεις, καθιστούν αναγκαίο τον σχεδιασμό και την εφαρμογή πολιτικών επιχειρησιακής συνέχειας. Ένα πανεπιστήμιο οφείλει να διασφαλίζει ότι οι βασικές του λειτουργίες (εκπαιδευτικές, ερευνητικές, διοικητικές) μπορούν να συνεχιστούν ακόμη και υπό συνθήκες κρίσης ή διακοπής.

Η υιοθέτηση ολοκληρωμένων μέτρων φυσικής και λειτουργικής ασφάλειας, σε συνδυασμό με ένα τεκμηριωμένο σχέδιο επιχειρησιακής συνέχειας, ενισχύει την ανθεκτικότητα του ιδρύματος, προάγει την εμπιστοσύνη της ακαδημαϊκής κοινότητας και εξασφαλίζει τη μακροπρόθεσμη σταθερότητα και αποστολή του πανεπιστημίου προς όφελος της κοινωνίας.

17.1. Φυσική ασφάλεια υποδομών

Σύμφωνα με τις διεθνείς καλές πρακτικές και τις προβλέψεις του ISO22301, θα πρέπει το προσωπικό και οι υποδομές να είναι προετοιμασμένες για μια σειρά διαφορετικών συμβάντων που ενδέχεται να θέσουν σε κίνδυνο την σωματική ακεραιότητα των εργαζομένων ή να προκαλέσουν προβλήματα στην λειτουργία των datacenters και των παρεχόμενων υπηρεσιών,

ως προς τη διαθεσιμότητά τους, ή ως προς την ακεραιότητα και εμπιστευτικότητα των δεδομένων τους.

Παρακάτω παρατίθεται η λίστα των συμβάντων και κρίσεων για τις οποίες θα πρέπει να υπάρχει πλάνο αντιμετώπισης, καθώς και σύντομες προτάσεις που προέρχονται από τις πρακτικές που υιοθετεί το ΑΠΘ.

17.1.1. Φυσικές καταστροφές

Σε αυτή την κατηγορία εντάσσονται σεισμοί, πλημμύρες και πυρκαγιές. Ως προς τις πυρκαγιές, θα πρέπει τα γραφεία των εργαζομένων να διαθέτουν επαρκή πυροσβεστικά μέσα και έξοδο κινδύνου ιδανικά προς εξωτερική σκάλα του κτηρίου για ασφαλή διαφυγή.

Σχετικά με τις προτεραιότητες που αφορούν σε υποδομές, δεδομένα και υπηρεσίες, θα πρέπει αν υπάρχουν πολλαπλά datacenters, αυτά να έχουν αναπτυχθεί σε σημεία που είναι φυσικώς απομακρυσμένα μεταξύ τους, ώστε να μην είναι δυνατόν μια πυρκαγιά που θα εκδηλωθεί σε οποιοδήποτε σημείο να προκαλέσει ταυτόχρονη καταστροφή πολλαπλών datacenters. Ταυτόχρονα, σε όλα τα datacenters θα πρέπει να υπάρχουν εγκατεστημένα αυτόματα συστήματα πυρόσβεσης για τον περιορισμό των ζημιών σε περίπτωση πυρκαγιάς.

Ως προς το ενδεχόμενο πλημμύρας, εάν η μορφολογία της τοποθεσίας στην οποία βρίσκεται το datacenter διατρέχει κίνδυνο πλημμύρας, θα πρέπει να έχουν γίνει οι αντίστοιχες μέριμνες για αντλίες, ψευδοπατώματα, υπερυψωμένα πεζούλια στις εισόδους, υδατοστεγείς πόρτες κλπ. Σε κάθε περίπτωση, θα πρέπει να υπάρχει τουλάχιστον μία εγκατάσταση ανιχνευτών πλημμύρας για έγκαιρη ειδοποίηση σε περίπτωση που κάποιο πλημμυρικό φαινόμενο είναι σε εξέλιξη.

Απεναντίας με τα προηγούμενα, το ενδεχόμενο ενός ισχυρού σεισμού δεν μπορεί να αποκλειστεί. Σχετικά με την διασφάλιση της σωματικής ακεραιότητας των εργαζομένων, θα πρέπει να υπάρχουν ευχερείς οδοί διαφυγής όπως περιγράφηκε και για την περίπτωση της πυρκαγιάς. Σε έναν ισχυρό σεισμό, υπάρχει η πιθανότητα να υπάρξει ευρύτερη καταστροφή που θα αφορά ολόκληρη περιοχή, συνεπώς ιδανικά θα πρέπει να υπάρχει τουλάχιστον ένα εφεδρικό datacenter σε φυσικώς απομακρυσμένο σημείο από το πρωτεύον datacenter.

17.1.2. Διακοπές/προβλήματα ηλεκτροδότησης

Τα προβλήματα στην ηλεκτροδότηση είναι τα πλέον συνηθισμένα και συνήθως είναι δύο τύπων: διακοπές ρεύματος (είτε προγραμματισμένες, είτε λόγω βλαβών), ενίοτε πολύωρες, και προβλήματα στην παρεχόμενη τάση (brownouts, spikes κλπ.). Τα προβλήματα της δεύτερης κατηγορίας αντιμετωπίζονται με online UPS τα οποία θα πρέπει να εξυπηρετούν το σύνολο

του ηλεκτροδοτούμενου εξοπλισμού σε όλα τα datacenters. Τα προβλήματα της πρώτης κατηγορίας αντιμετωπίζονται με τον συνδυασμό των UPS και ηλεκτρογεννητριών. Σε περίπτωση διακοπής ρεύματος, αναλαμβάνουν αρχικά τα UPS την υποστήριξη του εξοπλισμού και μέσα σε λίγα λεπτά με χρήση ειδικών ηλεκτρικών πινάκων αυτόματης μεταγωγής θα πρέπει να γίνεται αυτόματη εκκίνηση της τοπικής γεννήτριας, ώστε να υποστηριχθεί ο εξοπλισμός ακόμα και αν πρόκειται η διακοπή να διαρκέσει πολλές ώρες ή και ημέρες. Ιδανικά θα πρέπει να υπάρχει και μετρητής στάθμης καυσίμου ώστε να είναι ανά πάσα στιγμή γνωστή η επάρκεια των γεννητριών σε καύσιμο.

Θα πρέπει να σημειωθεί ότι επειδή ο κλιματισμός είναι απαραίτητος για την λειτουργία ενός datacenter, οι μονάδες κλιματισμού θα πρέπει να είναι κι αυτές συνδεδεμένες στη γεννήτρια (αλλά όχι στα UPS), συνεπώς οι γεννήτριες θα πρέπει να είναι κατάλληλα διαστασιολογημένες.

Επίσης, τυχόν άλλα κεντρικά σημεία διανομής στο δίκτυο (σε περιπτώσεις μεγάλων campuses) τα οποία είναι εκτός των κεντρικών datacenters, θα πρέπει κι αυτά να υποστηρίζονται από κατάλληλα UPS.

17.1.3. Τρομοκρατικές επιθέσεις & κλοπές

Η παρούσα κατηγορία καταστροφών περιλαμβάνει τις περιπτώσεις στοχευμένων φυσικών επιθέσεων εναντίον ζωτικών υποδομών του ιδρύματος. Για την αποτροπή τέτοιου είδους επιθέσεων, κάθε ίδρυμα θα πρέπει να εφαρμόζει αυστηρά πρωτόκολλα πρόσβασης στα datacenter του, αλλά και στα γραφεία του. Ιδανικά, τα γραφεία και ο εξοπλισμός των datacenters θα πρέπει να προστατεύονται από θωρακισμένες πόρτες, πρόσβαση με κάρτες RFID και καταγραφή εισόδων (τουλάχιστον για τα datacenters), συναγερμό με ανιχνευτές κίνησης και αυτόματη ενημέρωση της υπηρεσίας φύλαξης του ιδρύματος, κάγκελα στα παράθυρα, και κλειστό κύκλωμα βιντεοεπιτήρησης (CCTV), του οποίου το υλικό να αποθηκεύεται ταυτόχρονα σε δύο datacenters.

Εάν είναι δυνατό, τουλάχιστον το εφεδρικό datacenter θα πρέπει να μην είναι ευρέως γνωστό το που βρίσκεται. Εάν βρίσκεται σε κτήριο όπου συχνά παρευρίσκονται τρίτοι, θα πρέπει να μην έχει στην είσοδό του κάποια σήμανση/ταμπέλα που να καθιστά προφανές τι είναι.

Στην περίπτωση που οι θέσεις εργασίας (workstations) είναι κεντρικά διαχειρίσιμες από την υπηρεσία IT του ιδρύματος, θα πρέπει να είναι ενεργοποιημένη σε όλες η κρυπτογράφηση δίσκων (LUKS/Bitlocker), ώστε σε περίπτωση κλοπής να μην διαρρεύσουν ευαίσθητα δεδομένα που αφορούν ενδεχομένως σε φοιτητές, βαθμολογίες κλπ. Επιπλέον, ιδανικά θα πρέπει να μην υπάρχουν τοπικά αποθηκευμένα δεδομένα στις θέσεις εργασίας, αλλά να γίνεται χρήση κεντρικών αποθηκευτικών χώρων της υποδομής του ιδρύματος, ώστε είτε σε περίπτωση

κλοπής, είτε σε περίπτωση βλάβης της θέσης εργασίας να μπορεί να συνεχιστεί απρόσκοπτα η εργασία από άλλο υπολογιστή.

Τέλος, στα ιδρύματα συχνό είναι και το φαινόμενο καταλήψεων κτηρίων για μεγάλα χρονικά διαστήματα οπότε και οι διοικητικοί υπάλληλοι δεν έχουν φυσική πρόσβαση στους Η/Υ. Για να διασφαλίζεται η επιχειρησιακή συνέχεια του ιδρύματος, η υπηρεσία IT είναι απαραίτητο να διαθέτει υποδομές Remote Desktop Servers, ώστε να μπορεί να υπάρχει απρόσκοπτα πρόσβαση του συνόλου των χρηστών στα αρχεία και τις εφαρμογές τους για τέτοιες περιπτώσεις.

17.2. Λειτουργική ασφάλεια υποδομών

Στην παρούσα ενότητα παρουσιάζονται οι προτάσεις του ΑΠΘ ως προς τα συμβάντα που μπορούν να επηρεάσουν την υποδομή των ψηφιακών υπηρεσιών ενός ιδρύματος και για τα οποία θα πρέπει να έχει εφαρμοστεί κάποια στρατηγική αντιμετώπισης.

17.2.1. Τεχνολογικές αστοχίες

Στην κατηγορία αυτή ανήκουν αστοχίες υλικού καθώς και λογισμικού. Ως προς τις αστοχίες υλικού, θα πρέπει να υπάρχουν εφεδρείες τόσο σε επίπεδο δικτυακού εξοπλισμού και εξοπλισμού υποδομής servers από την οποία παρέχονται οι υπηρεσίες, όσο και σε επίπεδο συνολικά των datacenter, με αποτέλεσμα να υπάρχει πλήρης κάλυψη έναντι βλάβης σε οποιοδήποτε σύστημα.

Ως προς τις αστοχίες λογισμικού, αυτές μπορεί να προκύψουν από αναβαθμίσεις που δεν ολοκληρώθηκαν σωστά, ή από αλλαγές σε λογισμικό, οι οποίες περιείχαν bugs. Τέτοιου είδους προβλήματα είναι πολύ συνηθισμένα και αντιμετωπίζονται με διάφορους τρόπους. Ενδεικτικά, κάποια αποτυχημένη αναβάθμιση μπορεί άμεσα να ανακληθεί με χρήση της λειτουργικότητας των snapshots που υπάρχει διαθέσιμη στους hypervisors των εικονικών μηχανών, ενώ οι λοιπές αποτυχίες λογισμικού μπορούν να αντιμετωπιστούν με τη χρήση των αντιγράφων ασφαλείας που λαμβάνονται καθημερινά (ή και συχνότερα σε κάποιες περιπτώσεις).

17.2.2. Ανθρώπινα λάθη, ιοί και εσωτερικές απειλές

Ως προς τις κατηγορίες απειλών που μπορούν να επηρεάσουν την λειτουργική ασφάλεια των υποδομών, οι οποίες περιλαμβάνουν τα ανθρώπινα λάθη, τους ιούς και τις εσωτερικές απειλές, οι προτάσεις του ΑΠΘ περιλαμβάνουν τη λήψη αυτοματοποιημένων backups και snapshots των δεδομένων, καθώς και την καθολική εφαρμογή της αρχής του ελαχίστου δικαιώματος,

ώστε οτιδήποτε να συμβεί να μην είναι δυνατόν να επηρεάσει μεγάλο μέρος ή και το σύνολο της υποδομής. Οι λεπτομέρειες υλοποίησης παρατέθηκαν στις προηγούμενες ενότητες.

17.2.3. Κυβερνοεπιθέσεις

Ως προς τις κυβερνοεπιθέσεις εναντίον της λειτουργικής ασφάλειας των υποδομών, θα πρέπει το δίκτυο να είναι χωρισμένο σε VLANs ανά λογική οντότητα του ιδρύματος και ανά απαίτηση ασφαλείας κάθε οντότητας. Ειδικά για τις οντότητες υψηλού ρίσκου (π.χ. Γραμματείες), η πολιτική firewall θα πρέπει να είναι deny by default. Παρομοίως και για τα VLANs όπου βρίσκονται οι servers των ψηφιακών υπηρεσιών του ιδρύματος.

Επιπλέον θα πρέπει να εφαρμόζεται συνεχής παρακολούθηση της δικτυακής δραστηριότητας μέσω ελέγχου των NetFlow δεδομένων ή εναλλακτικά θα πρέπει να υπάρχει next generation firewall ώστε να μπλοκάρεται αυτόματα η προβληματική κίνηση και να ανιχνεύεται με DPI κάθε απόπειρα να περάσει στο δίκτυο πακέτο με virus signature.

Άλλου είδους απειλές οι οποίες μπορεί να θέσουν εκτός λειτουργίας τις υπηρεσίες που παρέχει το ίδρυμα είναι τα (Distributed) Denials of Service. Κατά την επίθεση με (D)DoS, οι υπηρεσίες καταρρέουν μέσω της επιβάρυνσής τους με ρυθμό αιτημάτων που η υποδομή δεν μπορεί να διαχειριστεί. Οι απλούστερες απειλές αυτού του είδους ανιχνεύονται εύκολα και αναχαιτίζονται αυτόματα από συστήματα προστασίας που μπορεί να αναπτύξει κάθε ίδρυμα (το ΑΠΘ στο παρελθόν έχει παραδώσει σεμινάρια και σχετικό κώδικα για υλοποίηση τέτοιων συστημάτων, στο πλαίσιο του έργου ΗΦΑΙΣΤΟΣ).

Ωστόσο για τις Distributed DoS επιθέσεις απαιτείται εξειδικευμένη προσέγγιση. Στις DDoS επιθέσεις τα αιτήματα προέρχονται από εκατοντάδες ή και χιλιάδες IP από όλο τον κόσμο, με αποτέλεσμα να μην είναι δυνατόν να ξεχωρίσουν τα πραγματικά αιτήματα προς την υπηρεσία από τα αιτήματα που γίνονται με σκοπό να την θέσουν εκτός λειτουργίας. Τέτοιου είδους επιθέσεις μπορούν να αντιμετωπιστούν μόνο από next-generation firewalls. Θα πρέπει επίσης να σημειωθεί ότι για ορισμένες υπηρεσίες, υπάρχει και άλλος ένας τρόπος προστασίας, που είναι το να προστατευθούν οι υπηρεσίες πίσω από κάποιον εμπορικό πάροχο διανομής περιεχομένου (Content Delivery Network – CDN) με χρήση αντίστοιχης συνδρομής. Για την ώρα, οι ελάχιστες μέσα στα χρόνια τέτοιου είδους επιθέσεις δεν έχουν καταστήσει απαραίτητη την επιδίωξη μιας τέτοιας λύσης και την συνεπαγόμενη οικονομική επιβάρυνση.

Επίσης, θα πρέπει τακτικά να διενεργούνται έλεγχοι ευπαθειών (με εργαλεία όπως Nessus, OpenVAS και αντίστοιχα), όλων των υπηρεσιών και εξυπηρετητών που είναι εκτεθειμένοι στο internet, αλλά και των εσωτερικών συστημάτων. Στη συνέχεια θα πρέπει τα ευρήματα να αντιμετωπίζονται ξεκινώντας από αυτά που ενέχουν το μεγαλύτερο ρίσκο για δεδομένα και υπηρεσίες.

Σε περιπτώσεις παραβίασης λογαριασμών και υποκλοπής στοιχείων και δεδομένων χρηστών, το ίδρυμα θα πρέπει να απενεργοποιεί άμεσα τους επίμαχους λογαριασμούς και να ειδοποιεί τους χρήστες για το συμβάν, ενώ θα πρέπει να εξετάζονται και οι υποχρέωσεις που απορρέουν από τον Γενικό Κανονισμό για την Προστασία των Δεδομένων (ΓΚΠΔ – GDPR). Για την αποφυγή τέτοιων περιστατικών, θα πρέπει να εφαρμόζεται όπου είναι δυνατόν MFA, καθώς και να ελέγχονται οι κωδικοί των χρηστών ως προς την επαρκή ασφάλειά τους. Ταυτόχρονα, θα πρέπει οπωσδήποτε να υπάρχουν μηχανισμοί αποτροπής του brute force κωδικών με εισαγωγή χρονοκαθυστέρησης ή/και μπλοκαρίσματος λογαριασμών.

17.2.4. Διαταραχές στην εφοδιαστική αλυσίδα

Στην κατηγορία αυτή ανήκουν τα προβλήματα που μπορεί να εμφανιστούν, εάν κάποιος κύριος προμηθευτής υλικού ή υπηρεσιών στις οποίες βασίζεται το ίδρυμα για να παράσχει τις υπηρεσίες του προς τους χρήστες του, δεν μπορεί πια να συνεχίσει να προμηθεύει υλικό ή υπηρεσίες. Στην περίπτωση του υλικού, το πρόβλημα αντιμετωπίζεται ήδη με όσα έχουν αναφερθεί στην ενότητα για την φυσική ασφάλεια. Συγκεκριμένα, με τις διαθέσιμες εφεδρείες που θα πρέπει να υπάρχουν και έχουν περιγραφεί, δεν υπάρχει εξάρτηση από κάποιον προμηθευτή εξοπλισμού και υλικών που να μπορεί να προκαλέσει άμεσο ή και μεσοπρόθεσμο πρόβλημα στην παροχή υπηρεσιών εκ μέρους του ιδρύματος, αν για οποιοδήποτε λόγο ο προμηθευτής διακόψει την λειτουργία του.

Σχετικά με τις εξαρτήσεις από υπηρεσίες τρίτων, θα πρέπει να αναφερθεί ότι όποια υπηρεσία μπορεί να αναπτυχθεί εσωτερικά στο ίδρυμα και να παρέχεται από τις υποδομές του, είναι προτιμότερη από υπηρεσία που αγοράζεται από τρίτους, τόσο για λόγους κόστους, όσο και για λόγους διατήρησης της αυτοτέλειας του ιδρύματος και της ανοχής του απέναντι σε διαταραχές στην εφοδιαστική αλυσίδα. Στην περίπτωση που πρέπει να παρέχεται υπηρεσία στην ιδρυματική κοινότητα από κάποιον τρίτο, θα πρέπει να υπάρχει πλάνο διεξόδου (π.χ. εναλλακτικός πάροχος) στην περίπτωση που ο τρέχων πάροχος της υπηρεσίας διακόψει την υπηρεσία ή αλλάξει δραματικά την τιμολογιακή του πολιτική.

Εδώ πρέπει να αναφερθεί και μια επιπλέον περίπτωση που αφορά άμεσα στην ασφάλεια αλλά και την επιχειρησιακή συνέχεια των ιδρυμάτων. Η τάση μετάβασης στο cloud, δηλαδή σε υπολογιστικές υποδομές και υπηρεσίες τρίτων, μπορεί υπό συνθήκες να προκαλέσει την αδυναμία πρόσβασης των ιδρυμάτων στις βάσεις δεδομένων γνώσεών τους, στα ticketing συστήματά τους και σε εσωτερικά έγγραφα, σε περίπτωση που συμβεί μια σοβαρή παραβίαση ασφαλείας στον πάροχο των υπηρεσιών ή σε αιφνίδια αλλαγή της τιμολογιακής πολιτικής ή ακόμα και αν κάποια κυβερνοεπίθεση θέσει εκτός λειτουργίας τον πάροχο της υπηρεσίας. Επίσης, πλέον τα δεδομένα όλων των χρηστών που αποθηκεύονται σε υπολογιστικές υποδομές τρίτων θα πρέπει να θεωρείται ότι δυνητικά αποτελούν υλικό για AI training, είτε εν γνώσει και με τη συναίνεση των ιδρυμάτων είτε όχι. Αυτό μπορεί να οδηγήσει σε διαρροές δεδομένων,

ενδεχομένως ευαίσθητων που μπορεί να αφορούν στην εσωτερική δομή των υπηρεσιών του ιδρύματος, στα συστήματα ασφαλείας κλπ. Και εδώ η σύσταση είναι ότι πρέπει κατά το δυνατόν να χρησιμοποιούνται οι υποδομές του ιδρύματος και οι εσωτερικές υπηρεσίες τους για την εξυπηρέτηση των αναγκών τους.

17.3. Επιχειρησιακή Συνέχεια

Αναλόγως με τις επιχειρησιακές προτεραιότητες του κάθε ιδρύματος, απαιτείται μια σαφής και τεκμηριωμένη πολιτική επιχειρησιακής συνέχειας που να καθορίζει πώς διασφαλίζεται η απρόσκοπτη λειτουργία κρίσιμων υπηρεσιών σε περίπτωση διαταραχής. Η πολιτική αυτή θα πρέπει να προσδιορίζει:

- ποιες λειτουργίες θεωρούνται κρίσιμες για την ακαδημαϊκή, ερευνητική και διοικητική αποστολή του ιδρύματος,
- ποια είναι τα αποδεκτά επίπεδα διακοπής ή υποβάθμισης υπηρεσιών,
- ποιοι ρόλοι και μηχανισμοί ενεργοποιούνται όταν προκύπτουν περιστατικά που απειλούν τη συνέχεια λειτουργίας,
- και ποια μέτρα προετοιμασίας, πρόληψης και γρήγορης αποκατάστασης απαιτούνται.

Για να είναι αποτελεσματική, η πολιτική επιχειρησιακής συνέχειας πρέπει να στηρίζεται σε συστηματική ανάλυση κινδύνων, να επικαιροποιείται τακτικά, να έχει την έγκριση της ανώτατης Διοίκησης και να ενσωματώνεται στον καθημερινό τρόπο λειτουργίας του ιδρύματος. Σκοπός δεν είναι μόνο η διαχείριση έκτακτων περιστατικών, αλλά η δημιουργία ενός ανθεκτικού οργανισμού που μπορεί να ανταποκριθεί σε κρίσεις χωρίς να υπονομεύεται ο ακαδημαϊκός του ρόλος.

Σε κάθε περίπτωση, δεδομένου του ότι πλέον στα ιδρύματα τόσο η επιτέλεση των ακαδημαϊκών υποχρεώσεων όσο και των διοικητικών γίνεται μέσα από τις υποδομές ψηφιακών υπηρεσιών, θα πρέπει κάθε ίδρυμα να διαθέτει εφεδρικές υποδομές, τουλάχιστον για τις κύριες υπηρεσίες του, και σίγουρα για το σύνολο των κρίσιμων δεδομένων του. Συνεπώς εάν οι υποδομές βρίσκονται συγκεντρωμένες σε ένα κεντρικό datacenter, θα πρέπει να υπάρχει άλλο ένα datacenter επαρκούς υπολογιστικής ισχύος ώστε να μπορεί να υποστηρίξει τις κρίσιμες υπηρεσίες. Επίσης, στο εφεδρικό datacenter θα πρέπει να γίνεται κατά το δυνατόν σε πραγματικό χρόνο αντιγραφή των δεδομένων του πρωτεύοντος datacenter, ώστε σε περίπτωση καταστροφής να μην υπάρξει απώλεια δεδομένων. Αυτό είναι χαρακτηριστικό το οποίο μια σύγχρονη enterprise αποθηκευτική συστοιχία μπορεί να υποστηρίξει.

Τέλος, σημαντικό είναι οι εφεδρείες των υποδομών να δοκιμάζονται συστηματικά, με όσο το δυνατόν πιο κοντά στην πραγματικότητα σενάρια. Στο ΑΠΘ κάθε δύο χρόνια εκτελείται μία

άσκηση ετοιμότητας κατά την οποία προσομοιώνεται η καταστροφή του πρωτεύοντος datacenter με κλείσιμο των παροχών των κεντρικών UPS που τροφοδοτούν όλο τον εξοπλισμό (routers, switches, blade servers, αποθηκευτικές συστοιχίες κλπ.). Έτσι ελέγχεται η καλή λειτουργία των εφεδρικών υποδομών και προκύπτουν προτάσεις για βελτιώσεις και συνεχή αύξηση του επιπέδου ετοιμότητας.