1. Εισαγωγή

Οι εξωτερικές απειλές χρειάζονται μια και μόνη επιτυχημένη προσπάθεια για να προκαλέσουν σοβαρή ζημιά στα απόρρητα δεδομένα ενός οργανισμού, πλήττοντας την ικανότητα του να παρέχει κρίσιμες υπηρεσίες ή την εταιρική φήμη του. Συνεπώς ο ΟΒΙ οφείλει να αναπτύσσει και να εξελίσσει μηχανισμούς πρόβλεψης κακόβουλων εισβολών και να επιταχύνει τον εντοπισμό των κινδύνων ώστε να προστατέψει τα εμπιστευτικά δεδομένα του. Για να αναγνωρίσει επιτυχώς και να αποκαταστήσει τις παρατεταμένες μη εξουσιοδοτημένες προσβάσεις στο δίκτυο του, που είναι γνωστές και ως AdvancedPersistentThreats – APTs, ο ΟΒΙ θα πρέπει να είναι προετοιμασμένος:

- Να χειρίζεται και να επεξεργάζεται πληροφορίες υψηλής ταχύτητας, μεγάλες σε όγκο και ποικιλία.
- Να αναλύει δομημένα και μη δομημένα δεδομένα τόσο εντός όσο και εκτός του δικτύου του.
- Να παρακολουθεί τα περιστατικά στο φυσικό και στο εικονικό περιβάλλον
- Να αναλαμβάνει δράση αυτόματα μόλις εντοπιστεί μια απειλή.

2. Αντικείμενο του έργου

Η παροχή εξειδικευμένων εξωτερικών υπηρεσιών διαχείρισης των απειλών ενάντια στα πληροφοριακά συστήματα του ΟΒΙ.

3. Τεχνική Περιγραφή

Στο πλαίσιο της προστασίας ο ΟΒΙ διενεργεί έρευνα αγοράς με σκοπό την παροχή εξωτερικών υπηρεσιών διαχείρισης της ασφαλείας (managed security services). Οι υπηρεσίες που θα πρέπει να παρέχει ο Ανάδοχος είναι οι ακόλουθες:

- Παρακολούθηση και Διαχείριση των Περιστατικών ασφαλείας
- Επικαιροποίηση της Μελέτης Ασφαλείας
- Αναβάθμιση του λογισμικού Bull Web Application Firewall
- Διαχείριση των συστημάτων ασφαλείας (Checkpoint UTM, Clear swift MIME Sweeper for SMTP, Bull Web Application Firewall)
- Συμβουλευτικές Υπηρεσίες

3.1 Παρακολούθηση και Διαχείριση των Περιστατικών ασφαλείας

Ο ΟΒΙ επιθυμεί τη συνεχή παρακολούθηση της υποδομής του σε σχέση με το επίπεδο ασφάλειας και την ενημέρωση για πιθανά συμβάντα ασφάλειας που σχετίζονται με αυτήν σε 24ωρη βάση. Για το λόγο αυτό ο Ανάδοχος θα πρέπει να προτείνει υποχρεωτικά υπηρεσία παρακολούθησης της ασφάλειας της υποδομής μέσω της υφιστάμενης πλατφόρμας IBMQRadar που διαθέτει ο ΟΒΙ. Τον έλεγχο και την άμεση ενημέρωση για τα περιστατικά ασφαλείας θα τον έχει ο Ανάδοχος.

Επιπρόσθετα, ο ΟΒΙ θα πρέπει να έχει πλήρη πρόσβαση σε όλα τα αρχεία καταγραφής συμβάντων (logfiles) σε πραγματικό χρόνο.

Μέσω της εν λόγω υπηρεσίας, ο ΟΒΙ θα ενημερώνεται άμεσα και σε πραγματικό χρόνο για κάθε συμβάν που αφορά σε θέματα ασφάλειας και έχει εντοπίσει ο ανάδοχος. Παράλληλα, τα εν λόγω συμβάντα/ Logs θα παραμένουν online για χρονική διάρκεια τριών μηνών και παράλληλα θα αρχειοθετούνται για χρονική διάρκεια έξι μηνών. Καθ' όλη τη διάρκεια αυτή θα πρέπει να είναι στη διάθεση του ΟΒΙ. Μέσω της εν λόγω υπηρεσίας ο Ανάδοχος θα συλλέγει τα συμβάντα από όλες τις εμπλεκόμενες συσκευές (δικτυακές ενσύρματες ή

ασύρματες, εξοπλισμό πιστοποίησης χρηστών, εξοπλισμό ασφάλειας όπως Firewall, κ.α.) καθώς επίσης και τη δικτυακή κίνηση.

Τη συλλογή θα ακολουθεί η επεξεργασία και ο συσχετισμός τους για την αναγνώριση πιθανών περιστατικών ασφάλειας και την κατηγοριοποίηση τους σε διαβαθμίσεις ανάλογα με την κρισιμότητά τους και τις πιθανές επιπτώσεις στην υποδομή του ΟΒΙ. Η συλλογή και επεξεργασία των σχετικών πληροφοριών θα γίνεται σε κατάλληλη υποδομή του αναδόχου (SecurityOperationCenter) από μηχανικούς που διαθέτουν κατάλληλες πιστοποιήσεις σε λογισμικό Checkpoint και QRadar. Ο ΟΒΙ θα πρέπει να ενημερώνεται για πιθανά περιστατικά ασφάλειας σε βάση μέσω e-mail,smsή τηλεφωνικής κλήσης ανάλογα με την κρισιμότητά τους.

Επιπρόσθετα θα πρέπει να μπορεί να παρακολουθεί τα εν λόγω περιστατικά μέσω WebPortal που θα αναπτύξει σχετικά ο ανάδοχος καθώς και να έχει πρόσβαση σε όλα τα αρχεία καταγραφής (logs).

Ο Ανάδοχος οφείλει να εκπαιδεύσει τον ΟΒΙ στη χρήση του Portal και της πλατφόρμας συλλογής, επεξεργασίας και παρακολούθησης περιστατικών ασφάλειας με αναλυτικό πρόγραμμα εκπαίδευσης που θα υποβάλλει σχετικά στον ΟΒΙ. Ειδικότερα για περιστατικά ασφάλειας τα οποία χαρακτηρίζονται σαν ύψιστης κρισιμότητας και μπορεί να επιφέρουν ιδιαίτερα σημαντικές επιπτώσεις στις υποδομές του ΟΒΙ, απαιτείται τηλεφωνική ενημέρωση.

Σε κάθε περίπτωση κατά την ενημέρωση για ένα περιστατικό ασφάλειας θα πρέπει να περιγράφεται το περιστατικό και να παρέχονται συμβουλές για την αντιμετώπισή του.

Ο ανάδοχος, πλην της επιτόπιας επέμβασης και ενημέρωσης για τυχόν συμβάντα ασφαλείας, οφείλει να παραδίδει την κατάλληλη αναφορά σε μηνιαία βάση. Η αναφορά θα περιγράφει συμβάντα που έλαβαν χώρα, προτεινόμενες βελτιστοποιήσεις και ότι άλλο κρίνει χρήσιμο.

Η παροχή της υπηρεσίας παρακολούθησης και ενημέρωσης για περιστατικά ασφάλειας θα γίνεται μέσω Επιχειρησιακού Κέντρου Ασφαλείας του αναδόχου. Να περιγράφει η αρχιτεκτονική υλοποίησης.

3.2 Επικαιροποίηση της Μελέτης Ασφαλείας

Ο Ανάδοχος θα πρέπει να επικαιροποιήσει την μελέτη ασφαλείας σύμφωνα με τα νέα πληροφοριακά συστήματα που έχει εντάξει ο ΟΒΙ στο δίκτυο του, στο νέο περιβάλλον της επικινδυνότητας καθώς και σύμφωνα με το πρότυπο ISO/IEC 27001:2013.

Η μελέτη ασφαλείας που είχε εκπονηθεί αποτελείτε από την ακόλουθη θεματολογία:

- Αποτίμηση της επικινδυνότητας

- Πολιτική Ασφαλείας

- Σχέδιο Ασφάλειας

3.3 Αναβάθμιση του λογισμικού Bull Web Application Firewall

Ο Ανάδοχος θα πρέπει να αναβαθμίσει το λογισμικό ασφαλείας της συσκευής Bull web application Firewall έτσι ώστε να προστατεύει τις διαδικτυακές υποδομές του ΟΒΙ από τις σύγχρονες τεχνικές και μεθοδολογίες επίθεσης προς τα περιβάλλοντα Web.

3.4 Διαχείριση των συστημάτων ασφαλείας (Checkpoint UTM, Bull Web Application Firewall)

Ο Ανάδοχος θα πρέπει να παρέχει υπηρεσίες διαχείρισης και υποστήριξης των ακόλουθων συστημάτων ασφαλείας του ΟΒΙ:

- Checkpoint UTM,

- Bull Web Application Firewall

Οι υπηρεσίες υποστήριξης και διαχείρισης των συστημάτων ασφαλείας περιγράφονται και καθορίζονται παρακάτω:

- Υπηρεσίες Help Desk οι οποίες περιλαμβάνουν:
- Λήψη, καταγραφή και διαχείριση των κλήσεων για επίλυση προβλημάτων
- Τηλε-διάγνωση προβλημάτων χρήσης και λειτουργίας
- Τηλε-επίλυση προβλημάτων χρήσης και λειτουργίας στο λογισμικό ασφαλείας firewall, IDS, webapplicationfirewallκαι mimesweeper for SMTP
- Τηλε-βοήθεια προβλημάτων προς τους διαχειριστές για την αντιμετώπιση προβλημάτων
- Υπηρεσίες Τεχνικής Υποστήριξης που περιλαμβάνουν:
- Παρουσία τεχνικού της εταιρείας μας εντός (4) τεσσάρων ωρών, σε περίπτωση προβλήματος που δεν μπορεί να λυθεί μέσω HelpDeskγια On-Site διάγνωση και επίλυση τρεχόντων προβλημάτων στο λογισμικό ασφαλείας
- Εγκατάσταση διορθωτικών εκδόσεων (Patches, Releases, κλπ) που διαθέτουν οι εταιρείες κατασκευής του λογισμικού ασφαλείας. Οι διορθωτικές εκδόσεις θα παρέχονται στον Ανάδοχο από τον OBI.
- Παραμετροποίηση των συστημάτων ασφαλείας

3.5 Διάθεση εγκαταστάσεων για Υλοποίηση Σχεδίου Έκτακτης Ανάγκης (DRP)

Ο Ανάδοχος θα πρέπει να παρέχει ικανοποιητικό χώρο για την λειτουργία τουλάχιστον τριών σταθμών εργασίας και τους ανάλογους serversγια την λειτουργία των κεντρικών υπηρεσιών του OBI σε περίπτωση έκτακτης ανάγκης.

3.6 Συμβουλευτικές Υπηρεσίες

Ο Ανάδοχος θα πρέπει να παρέχει συμβουλευτικές υπηρεσίες σε θέματα ασφάλειας πληροφοριακών συστημάτων, όταν ζητείται από τους αρμόδιους του OBI και προφανώς όταν προκύπτουν απρόβλεπτα ζητήματα όπως:

• Επιβεβλημένη έκτακτη αλλαγή στοιχείων του πληροφοριακού συστήματος,

• Προσθήκη νέων υπηρεσιών ή τροποποίηση απαιτήσεων γι' αυτές που παρέχονται από το πληροφοριακό σύστημα,

• Αλλαγή δεδομένων σε ζητήματα ασφάλειας, λόγω τεχνολογικών εξελίξεων ή αντικατάσταση εξοπλισμού, που απαιτούν άμεση αντιμετώπιση,

• Εκτίμηση κόστους για την προμήθεια και υλοποίηση νέου εξοπλισμού για το σύστημα διασφάλισης του πληροφοριακού συστήματος.

• Hardening νέου εξοπλισμού για την διασφάλιση του πληροφοριακού συστήματος.

• Τουλάχιστον μια μελέτη ασφάλειας πληροφοριακών συστημάτων εφόσον παρουσιαστεί ανάγκη.

4. Ελάχιστες Προϋποθέσεις Συμμετοχής

- Ο Ανάδοχος θα πρέπει να διαθέτει ISO/IEC 27001 και να έχει υλοποιήσει τουλάχιστον τρία (3) παρόμοια έργα την τελευταία τριετία.

- Τα στελέχη του Αναδόχου θα πρέπει να διαθέτουν πιστοποίηση σε Checkpoint UTM ((Checkpoint Certified Security Experts) και σε λογισμικό QRadar.

- Ο Ανάδοχος θα πρέπει να διαθέτει Κέντρο Παρακολούθησης.