

Issue

Πόσο κινδυνεύουν οι ελληνικές επιχειρήσεις από περιστατικά παραβίασης συστημάτων & απώλειας δεδομένων;

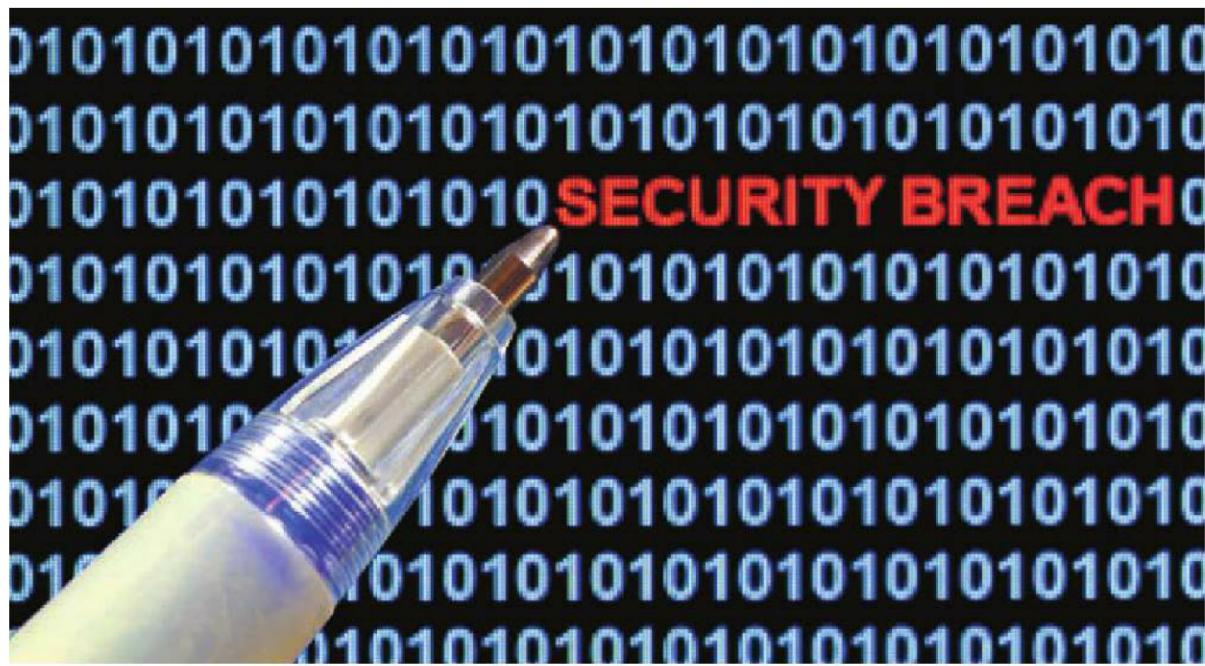


ύμφωνα με τον **Ντέιβιντ Εμ**, επικεφαλής αναλυτής Ασφάλειας στην Παγκόσμια Ομάδα Έρευνας και Ανάλυσης της Kaspersky Lab, ο οποίος παρουσίασε στο Fortune τα πιο πρόσφατα ευρήματα, **τις τάσεις των κυβερνοεγκλημάτων** και τους τρόπους με τους οποίους κάθε εταιρεία μπορεί να προστατευτεί από αυτό που οι άνθρωποι του χώρου της ψηφιακής ασφάλειας χαρακτηρίζουν «αναπόφευκτο».

«Μέσα στο 2014, το 94% των επιχειρήσεων αντιμετώπισεν ζητήματα ψηφιακής ασφάλειας που προέρχονταν εκτός της εταιρείας και το 12% έπεισαν θύματα στοχευμένων επιθέσε-

ων» τονίζει ο Ντέιβιντ Εμ. «**Παγκοσμίως, το μέσο κόστος ενός περιστατικού παραβίασης δεδομένων ανέρχεται στα 720.000 δολάρια**. Ωστόσο, η έρευνα της Kaspersky για τις παγκόσμιες ψηφιακές προκλήσεις το 2014 έδειξε ότι το κόστος μιας επιτυχημένης στοχευμένης επίθεσης θα μπορούσε να φτάσει μέχρι και τα 2,54 εκατομμύρια δολάρια». Η Ελλάδα δεν αποτελεί εξαίρεση σε αυτήν τη «μάχη» για τη διασφάλιση των ευαίσθητων εταιρικών δεδομένων. Σύμφωνα με τα πιο πρόσφατα στοιχεία των Kaspersky Lab και B2B International, το 2013 το 96% των ελληνικών επιχειρήσεων αντιμετώπισεν ζητήματα ψηφιακής ασφάλειας.

Στην έρευνα της Kaspersky για τις ψηφιακές απειλές των





Nikos Georghiopoulos, MBA, CyRM.
Cyber Risk Advisor, www.cyberinsurancegreece.com
CROMAR Coverholder at LLOYD'S

ελληνικών εταιρειών το 2013:

- το 87% εξ αυτών αντιμετώπισαν εσωτερικά ζητήματα α-σφάλειας κυρίως λόγω απροσεξίας των εργαζομένων
- στο 39% των περιπτώσεων, η διαρροή δεδομένων οφειλόταν σε ανθρώπινο λάθος των στελεχών
- στο 18% στη λανθασμένη χρήση βασικών ψηφιακών υπο-ρειών από φορητές συσκευές («έξυπνα» κινητά, tablets).

Πρόληψη και διαχείριση περιστατικών παραβίασης συστημάτων και απώλειας δεδομένων

«Το σημείο εκκίνησης για κάθε επιχείρηση πρέπει να είναι η αξιολόγηση των κινδύνων», ορίζοντας τον τρόπο με τον οποίο πρέπει να κινηθεί κάθε εταιρεία που θέλει να διασφαλίσει την ψηφιακή παρουσία της. Οι βασικές ερωτήσεις που πρέπει να τεθούν από κάθε επιχειρηματία είναι οι εξής: Ποια περιουσιακά στοιχεία διαθέτει η επιχείρησή του (πνευματική ιδιοκτησία, δεδομένα πελατών κ.λπ.), ποιοι θα μπορούσαν να θέλουν να της επιτεθούν και με ποιον τρόπο θα επιχειρούσαν να τα κάνουν πράξη;

Λαμβάνοντας υπόψη τα παραπόνω «η επιχείρηση πρέπει να χαράξει μια στρατηγική για τον περιορισμό των κινδύνων. Αυτό περιλαμβάνει τη δημιουργία “άμυνας σε Βάθος”, αν υποθέσουμε ότι ένας εισβολέας μπορεί να προσπεράσει την περιμετρική άμυνα. Η τεχνολογία παιζει σημαντικό ρόλο, αλλά δεν αρκεί».

Δυστυχώς, υπάρχουν αρκετά παραδείγματα παραβιάσεων συστημάτων επιχειρήσεων που δεν ήταν επαρκώς προετοιμασμένες και δεν κατάφεραν να διαχειριστούν αποτελεσματικά τα εκδηλωθέντα περιστατικά.

Για το λόγο αυτό θα πρέπει σε κάθε εταιρία να έχει συσταθεί μια **Ομάδα Διαχείρισης Περιστατικών Παραβίασης Συστημάτων** η οποία αποτελείται από ανώτατα στελέχη της εταιρίας από τμήματα όπως:

- Information Security
- Πληροφορική
- Νομικη υπηρεσία
- Κανονιστική Συμμόρφωσης
- Επικοινωνίας
- Εξυπρέπησης Πελατών
- Οικονομική Διεύθυνση
- Business Continuity
- HR
- Marketing

και εξειδικευμένους εξωτερικούς συμβούλους όπως: δικογόρους, επικοινωνιολόγους, ερευνητές ψηφιακής εγκληματολογίας.

Η ομάδα πρέπει να συνεδριάζει σε τακτικά χρονικά διαστή-



ματα και να εκπονεί ασκήσεις προσομοίωσης διάφορων σεναρίων ώστε τα μέλη της να είναι σε ετοιμότητα για την αντιμετώπιση περιστατικών.

Η ομάδα αυτή πρέπει να συντονίζεται από τον **Cyber Breach Coach** ο οποίος θα φροντίζει για την συνεχή ετοιμότητα της και θα δίνει την κατάλληλη πληροφόρηση στον Διευθύνοντα Σύμβουλο κατά την εξέλιξη ενός περιστατικού παραβίασης. Όταν συμβεί παραβίαση συστημάτων και διαρροή δεδομένων, θα πρέπει να παρθούν γρήγορα αποφάσεις και πολλές φορές χωρίς δυνατότητα αναίρεσης ακόμα.

Η ασφάλιση Cyber Insurance ως Εργαλείο Διαχείρισης Περιστατικών Παραβίασης Συστημάτων.

Τα περιστατικά παραβίασης συστημάτων και απώλειας εμπιστευτικών πληροφοριών δημιουργούν άμεσες και έμμεσες δαπάνες οι οποίες είναι απραγματιστείς, έχουν αρνητική επίπτωση στην ρευστότητα και τις ταμειακές ροές ενός οργανισμού και επηρεάζουν τον Ισολογισμό της.

Η **Ασφάλιση Cyber Insurance** είναι ένα κρίσιμο κομμάτι της συνολικής στρατηγικής για τη διαχείριση των κινδύνων. Ενώ στον κυβερνοχώρῳ η ασφάλιση δεν μπορεί να εμποδίσει ένα περιστατικό ασφαλείας, μπορεί:

- να συμπληρώσει την **Ομάδα Διαχείρισης Περιστατικών Παραβίασης Συστημάτων** με την παροχή βοήθειας μέσω εξειδικευμένων παρόχων που παρέχουν τις κατάλληλες υποδομές και το κατάλληλο ανθρώπινο δυναμικό,
- να βοηθήσει στην καλύτερη διαχείριση των περιστατικών μειώνοντας τις επιπτώσεις της παραβίασης στους πελάτες, τη φήμη της εταιρίας,
- και να καλύψει το χρηματοοικονομικό κόστος του περιστατικού ώστε να μην επηρεαστούν τα χρηματοοικονομικά μεγέθη της εταιρίας. **IT Security**