Αποθήκευση δεδομένων & GDPR

Το GDPR έρχεται και το σύστημα αποθήκευσης σας θα πρέπει να είναι σε θέση να καλύψει όλες τις απαιτήσεις που θα προκύψουν. Θα πρέπει να διαθέτει την απαιτούμενη αξιοπιστία ώστε να προστατεύει τα πολύτιμα δεδομένα του οργανισμού παρέχοντας παράλληλα την απαιτούμενη απόδοση & επεκτασιμότητα στην εταιρική υποδομή. Θα πρέπει να μπορεί να ανταπεξέλθει στις ανάγκες αποθήκευσης που θα προκύψουν στο πλαίσιο συμμόρφωσης με τον κανονισμό του GDPR.

Η σημασία του σωστού προσδιορισμού

Το σύστημα αποθήκευσης, έπαιζε, παίζει & θα παίζει πρωταγωνιστικό ρόλο στην ομαλή & απρόσκοπτη λειτουργία κάθε εταιρικού περιβάλλοντος. Το σύστημα αποθήκευσης είναι ο πυρήνας της υποδομής & ο χώρος στο οποίο αποθηκεύεται ο πολυτιμότερος πόρος ενός οργανισμού, τα εταιρικά δεδομένα. Ανεξαρτήτως του μεγέθους της επιχείρησης & του πλήθους των δεδομένων που καλείται να προστατεύσει, η συνεισφορά του συστήματος αποθήκευσης στην λειτουργία ενός οργανισμού είναι καθοριστική. Το σύστημα αποθήκευσης θα πρέπει να μπορεί να διαθέτει τους απαιτούμενους πόρους (IOPS performance, & usable capacity) ώστε να καλύπτονται πλήρως όλες οι ανάγκες των εφαρμογών που καλείται να υποστηρίξει. Σε αντίθετη περίπτωση η λειτουργικότητα ενός

οργανισμού καθίσταται προβληματική, καθώς η έλλειψη του συγκεκριμένου πόρου, αποτελεί κρίσιμο παράγοντα για την ομαλή λειτουργία των εφαρμογών.

Το σύστημα αποθήκευσης θα πρέπει να είναι αξιόπιστό, να υποστηρίζει χαρακτηριστικά υψηλής διαθεσιμότητας & να προστατεύει αποτελεσματικά τα παραγωγικά δεδομένα του οργανισμού. Θα πρέπει να έχει όλα τα κρίσιμα στοιχεία του σε εφεδρεία ώστε να μην υπάρχει single point of failure στην υποδομή, το οποίο θα μπορούσε να μειώσει τον βαθμό διαθεσιμότητας των εφαρμογών και συνολικά της IT υποδομής.

Θα πρέπει επίσης το σύστημα να είναι επεκτάσιμό τόσο όσον αφορά την διασύνδεση του με τους εξυπηρετητές της υποδομής όσο και αναφορικά με την ωφέλιμη χωρητικότητα & το IOPS performance που καλείται να παράσχει στις εφαρμογές του οργανισμού. Το σύστημα θα πρέπει επίσης να μπορεί να υποστηρίξει τις αυξημένες ανάγκες ενός οργανισμό, όπως π.χ disaster recovery λειτουργικότητα παρέχοντας συγχρονισμό (σύγχρονο ή ασύγχρονο) με αντίστοιχο εξοπλισμό σε αλλά εταιρικά sites ή cloud providers επιτυγχάνοντας ακόμα μεγαλύτερα ποσοστά διαθεσιμότητας των εφαρμογών και της επιχειρηματικότητας στο σύνολο της .

Όλα τα ανωτέρω, αναδεικνύουν με τον καλύτερο τρόπο την σπουδαιότητα που έχει ένα τέτοιο σύστημα στο περιβάλλον ενός οργανισμού. Η είσοδος του κανονισμού GDPR, στην πραγματικότητα ενός οργανισμού, έρχεται να επιβαρύνει ακόμα περισσότερο τις ήδη αυξημένες αρμοδιότητες και υποχρεώσεις που έχει ένα σύστημα αποθήκευσης. Με την ολοκλήρωση της μελέτης για την συμμόρφωση με το πρότυπο του GDPR & την σύνταξη του GAP analysis report, θα προκύψουν ανάγκες για εφαρμογές που σκοπό θα έχουν να προστατεύσουν τον οργανισμό και τα δεδομένα αυτού από απειλές, επιτυγχάνοντας παράλληλα συμμόρφωση με το συγκεκριμένο πρότυπο. Οι επεξεργαστικές ανάγκες του οργανισμού θα πρέπει να αυξηθούν για να υποστηρίξουν τις απαιτούμενες εφαρμογές ασφάλειας (π.χ data classification & categorization, data loss prevention, data encryption, backup, antivirus & antispam solution κλπ) και η επεκτασιμότητα του συστήματος αποθήκευσης θα δοκιμαστεί καθώς θα πρέπει να ανταποκριθεί στις νέες αυξημένες ανάγκες.

GDPR Storage best practices

Προκειμένου να ανταποκριθούμε στις τεχνολογικές τάσεις του κανονισμού GDPR και να αντιμετωπίσουμε αποτελεσματικά τις αδυναμίες ασφάλειας, προτείνεται η εφαρμογή των παρακάτω κανόνων & βέλτιστων πρακτικών για την ασφάλεια των δεδομένων των οργανισμών:

1. Πολιτικές ασφάλειας αποθήκευσης δεδομένων: Οι οργανισμοί πρέπει να έχουν πολιτική που θα καθορίζει τα κατάλληλα επίπεδα ασφάλειας για τους διάφορους τύπους δεδομένων που διαθέτουν. Προφανώς, τα δημόσια δεδομένα χρειάζονται πολύ λιγότερη ασφάλεια από ό, τι τα εμπιστευτικά δεδομένα και ο οργανισμός

πρέπει να έχει πρότυπα ασφάλειας, διαδικασίες και εργαλεία για την εφαρμογή κατάλληλων προστατευτικών μέτρων. Οι πολιτικές θα πρέπει επίσης να περιλαμβάνουν λεπτομέρειες σχετικά με τα μέτρα ασφάλειας που πρέπει να εφαρμοστούν στις συσκευές αποθήκευσης που χρησιμοποιεί ο οργανισμός. Η κατηγοριοποίηση αυτή των δεδομένων σε κλάσεις & η εφαρμογή κατάλληλης πολιτικής ασφάλειας στα συγκεκριμένα δεδομένα, ανάλογα με την κλάση, είναι λειτουργικότητα απαραίτητη στο πλαίσιο συμμόρφωσης με το πρότυπο GDPR. Μέσω της συγκεκριμένης λειτουργικότητας διασφαλίζεται η προστασία των δεδομένων ανάλογα με τον βαθμό κρισιμότητα τους με ένα δομημένο τρόπο. Τέτοιου είδους εφαρμογές data classification συνήθως έχουν υψηλές ανάγκες σε IOps για να λειτουργήσουν ομαλά & να παράξουν αποτέλεσμα, επιβαρύνοντας σημαντικά το σύστημα αποθήκευσης κατά την διάρκεια της εκτέλεσης των εργασιών.

2. Έλεγχος πρόσβασης: Ο έλεγχος πρόσβασης των χρηστών στις εφαρμογές & στα αποθηκευμένα δεδομένα του οργανισμού πρέπει να γίνεται βάσει ρόλων & δικαιωμάτων, που ανατίθενται με βάση την εταιρική πολιτική ασφάλειας. Ανάλογα με τις ανάγκες ασφάλειας του οργανισμού, πολλές φορές είναι απαραίτητη η χρήση multi-factor ελέγχου πιστοποίησης. Κάποιες φορές είναι απαραίτητη η χρήση πλατφόρμας, μέσω της οποίας ελέγχονται και άλλες παράμετροι που εμπλέκονται στην πρόσβαση του εκάστοτε χρήστη στους εταιρικούς πόρους. Πχ το ενημερωμένο OS & antivirus engine του τερματικού, η ώρα, ο τύπος του τερματικού & το σημείο από το οποίο γίνεται η προσπάθεια πρόσβασης στους πόρους του οργανισμού είναι παράμετροι που πιθανά απαιτούν έλεγχο πριν επιτρέψουν την πρόσβαση σε κάποια εταιρικά περιβάλλοντα. Τέτοιου είδους λύσεις επιβαρύνουν το σύνολο της υποδομής IT του οργανισμού συμπεριλαμβανομένου και του συστήματος αποθήκευσης.

3. Κρυπτογράφηση: Τα δεδομένα του οργανισμού θα πρέπει να κρυπτογραφούνται τόσο κατά τη μεταφορά όσο και κατά την παραμονή τους στα συστήματα αποθήκευσης. Οι διαχειριστές αποθήκευσης πρέπει να διαθέτουν ασφαλές σύστημα διαχείρισης κλειδιών για την παρακολούθηση των κωδικών κρυπτογράφησης. Εξαιρετικά χρήσιμο θα ήταν, εάν το σύστημα αποθήκευσης, μπορούσε να υποστηρίζει την κρυπτογράφηση των εταιρικών δεδομένων, χωρίς επιβάρυνση της απόδοσης του, ώστε να μην χρειαστεί άλλη σχετική λύση για την προστασία των πολύτιμων δεδομένων. Πληθώρα λύσεων είναι διαθέσιμη σε αυτόν τον τομέα ανάλογα με τις ανάγκες της εκάστοτέ επιχείρησης. Οι δημοφιλέστερες εκ αυτών υλοποιούνται μέσω ενεργοποίησης της συγκεκριμένης δυνατότητας του συστήματος αποθήκευσης, το οποίο για τον σκοπό αυτό χρησιμοποιεί ξεχωριστά cpus ώστε η συγκεκριμένη λειτουργία να μην επιβαρύνει της πρωταρχική λειτουργικότητα του συστήματος.

4. Data loss prevention: Ίσως το σημαντικότερο εργαλείο στο πλαίσιο προφύλαξης των δεδομένων ενός οργανισμού. Σε στενή συνεργασία με την λειτουργικότητα data classification που αναφέρθηκε παραπάνω, η συγκεκριμένη πλατφόρμα αναλαμβάνει να εκτελέσει τις εταιρικές πολιτικές ώστε να προστατευθούν τα ευαίσθητα δεδομένα του οργανισμού. Τέτοιες λύσεις επιβαρύνουν το σύνολο της IT υποδομής συμπεριλαμβανομένου και του συστήματος αποθήκευσης.

5. Perimeter security systems: Η υποδομή IT & ειδικότερα το σύστημα αποθήκευσης θα πρέπει να προστατεύεται από ισχυρά συστήματα ασφάλειας δικτύων, όπως

firewalls, antispam & antimalware systems, intrusion protection systems κλπ. Τα συγκεκριμένα συστήματα είναι πολύ πιθανόν, εκμεταλλευόμενοι τα πλεονεκτήματα του virtualization, να τρέχουν ως ανεξάρτητα VMs πάνω στην υποδομή, και να χρησιμοποιούν τα χαρακτηριστικά υψηλής διαθεσιμότητας που αυτή υποστηρίζει. Με αυτόν τον τρόπο επιτυγχάνεται failover χωρίς την ανάγκη αγοράς ξεχωριστού εφεδρικού HW, αποκλειστικά για τον σκοπό αυτό. Τέτοιες λύσεις έχουν και αυτές με την σειρά τους αντίκτυπο στο σύστημα αποθήκευσης του οργανισμού.

6. Συστήματα endpoint security: Κάθε σταθμός εργασίας θα πρέπει να διαθέτει ένα ενημερωμένο & αξιόπιστό λογισμικό endpoint protection. Η συνήθης πρακτική είναι να υπάρχει κεντρικοποιημένη διαχείριση της υπηρεσίας, μέσω της οποίας & με βάση την εταιρική πολιτική να καλύπτονται τα τερματικά των χρηστών (μέσω push updates, antivirus scans κλπ). Και σε αυτή την περίπτωση υπάρχει αντίκτυπο στο σύστημα αποθήκευσης.

7. Backup & recovery: Η λήψη αντιγράφων ασφάλειας είναι απαραίτητη καθώς επιτρέπει την προστασία των δεδομένων & των εφαρμογών του οργανισμού με ένα δομημένο τρόπο. Τα αντίγραφα ασφάλειας λαμβάνονται σύμφωνα με την πολιτική του οργανισμού & την κρισιμότητα των δεδομένων που προστατεύουν. Υπάρχει πληθώρα λύσεων backup-restore ανάλογα με το μέγεθος & την πολυπλοκότητα του εταιρικού περιβάλλοντος. Ανάλογα με τις ανάγκες του οργανισμού επιλέγετε είτε backup σε tape είτε σε δίσκο είτε σε κάποιο συνδυασμό αυτών. Κάποιες φορές οι ανάγκες επιβάλουν από το σύστημα Backup replication/μεταφορά (είτε μέσω tape out) των backup δεδομένων και σε κάποιο άλλο site για μεγαλύτερη προστασία των δεδομένων του οργανισμού. Σε αυτές τις περιπτώσεις είναι επιβεβλημένη η προστασία των συγκεκριμένων δεδομένων με κάποια μέθοδο κρυπτογράφησης καθώς ο κίνδυνός να υποπέσουν ευαίσθητα δεδομένα σε λάθος χέρια είναι αυξημένος.

Ο σύμβουλος στην νέα εποχή

Σε κάθε περίπτωση η Cosmos διαθέτει την απαραίτητη τεχνογνωσία να υποστηρίξει τον οργανισμό σας σε όλα τα επίπεδα για την βέλτιστη μετάβαση σας στην μετά GDPR εποχή. Διαθέτει άρτια καταρτισμένους μηχανικούς τόσο σε presales όσο και σε after sales επίπεδο και συνεργάζεται με όλους του μεγάλους κατασκευαστές συστημάτων, ώστε να μπορεί να προτείνει & να υποστηρίξει πλήρως την βέλτιστη τεχνοοικονομική λύση, σύμφωνα με τις ιδιαίτερες ανάγκες & απαιτήσεις ενός οργανισμού. Με αυτόν τον τρόπο η μετάβαση στην νέα εποχή γίνεται εύκολα, συντεταγμένα & απροβλημάτιστα για τον οργανισμό σας. Η γνώση & η εμπειρία των στελεχών της εταιρείας Cosmos, καθοδηγούν τους πελάτες & συνεργάτες μας στο ταξίδι αυτό, αποφεύγοντας την υιοθέτηση λύσεων & προϊόντων τα οποία δεν είναι προς όφελος τους.