Η σημασία των αντιγράφων ασφαλείας

Βασικές έννοιες

Τύποι backup, κανόνες και μεθοδολογίες

Απειλές & κίνδυνοι

Ransomware, ανθρώπινα λάθη, επιχειρησιακή συνέχεια

Εργαλεία & πρακτικές

Cloud, NAS, κρυπτογράφηση, αυτοματοποίηση

Έλεγχος & ανάκαμψη

Restore testing, RPO/RTO, διαχείριση περιστατικών

Επιμελητήριο Ηρακλείου
Heraklion Chamber of Commerce & Industry
safeLine.gr
ΙΤΕ ΙΝΣΤΙΤΟΥΤΟ ΠΛΗΡΟΦΟΡΙΚΗΣ
Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

Γιατί τα backups είναι κρίσιμα

Η απώλεια δεδομένων δεν είναι απλώς τεχνικό πρόβλημα — είναι επιχειρηματικός κίνδυνος. Σύμφωνα με έρευνες, **το 60% των εταιρειών που χάνουν κρίσιμα δεδομένα κλείνουν εντός 6 μηνών**.

🔒 Ransomware

Κακόβουλο λογισμικό που κρυπτογραφεί δεδομένα και απαιτεί λύτρα. Χωρίς backup, η επιλογή είναι πληρωμή ή μόνιμη απώλεια.

💾 Απώλεια δεδομένων

Βλάβες hardware, ανθρώπινα λάθη, διαγραφές, φυσικές καταστροφές — κανένα σύστημα δεν είναι άτρωτο χωρίς αντίγραφα.

🏢 Επιχειρησιακή συνέχεια

Τα backups εξασφαλίζουν ότι η επιχείρηση μπορεί να συνεχίσει να λειτουργεί μετά από οποιοδήποτε συμβάν, ελαχιστοποιώντας το downtime.

Κυβερνοαπειλές που στοχεύουν τα δεδομένα σας

Το τοπίο των απειλών εξελίσσεται συνεχώς. Κατανοώντας τους τύπους επιθέσεων, μπορείτε να σχεδιάσετε αποτελεσματικότερη στρατηγική backup.

Ransomware

Κρυπτογραφεί αρχεία και απαιτεί λύτρα. Οι επιθέσεις έχουν αυξηθεί κατά 150% τα τελευταία χρόνια, στοχεύοντας κυρίως επιχειρήσεις.

Malware & trojans

Κακόβουλο λογισμικό που καταστρέφει, κλέβει ή παραποιεί δεδομένα, συχνά χωρίς ο χρήστης να αντιληφθεί αμέσως την επίθεση.

Insider threats

Εσωτερικοί χρήστες με κακόβουλη πρόθεση ή αμέλεια αποτελούν σημαντική πηγή απώλειας δεδομένων που συχνά υποεκτιμάται.

Ανθρώπινα λάθη

Κατά λάθος διαγραφές, εσφαλμένες ρυθμίσεις ή απροσεξία αποτελούν την πιο συχνή αιτία απώλειας δεδομένων σε επιχειρήσεις.

Business continuity & disaster recovery

Το **Σχέδιο Επιχειρησιακής Συνέχειας (BCP)** και το **Σχέδιο Αποκατάστασης από Καταστροφή (DRP)** αποτελούν αναπόσπαστο κομμάτι κάθε σύγχρονης στρατηγικής ασφάλειας. Τα backups είναι ο πυρήνας αυτών των σχεδίων.

Business Continuity Plan (BCP)

Διασφαλίζει ότι οι κρίσιμες επιχειρηματικές λειτουργίες συνεχίζονται κατά τη διάρκεια και μετά από ένα περιστατικό.

- Προσδιορισμός κρίσιμων συστημάτων
- Ορισμός εναλλακτικών διαδικασιών
- Εκπαίδευση προσωπικού
- Τακτικές δοκιμές και επικαιροποίηση

Disaster Recovery Plan (DRP)

Εστιάζει στην τεχνική αποκατάσταση συστημάτων και δεδομένων μετά από σοβαρό συμβάν.

- Καθορισμός RPO και RTO στόχων
- Διαδικασίες restore από backup
- Ιεράρχηση αποκατάστασης συστημάτων
- Επικοινωνία με stakeholders

Χωρίς τεκμηριωμένο σχέδιο και δοκιμασμένα backups, ακόμα και η καλύτερη τεχνολογία δεν αρκεί για αποτελεσματική αποκατάσταση.

Backup vs συγχρονισμός

Πολλές επιχειρήσεις πιστεύουν εσφαλμένα ότι εργαλεία συγχρονισμού όπως το Dropbox ή το OneDrive αντικαθιστούν το backup. **Αυτή είναι μια επικίνδυνη παρανόηση.**

Ο συγχρονισμός είναι εξαιρετικό εργαλείο για ομαδική εργασία, αλλά **δεν προστατεύει από ransomware, κατά λάθος διαγραφές ή καταστροφή δεδομένων**. Χρειάζεστε και τα δύο — με διαφορετικούς ρόλους.

Ο κανόνας 3-2-1

Ο κανόνας **3-2-1** είναι το θεμέλιο κάθε αξιόπιστης στρατηγικής backup. Απλός στη λογική, αποτελεσματικός στην πράξη.

3 Αντίγραφα

Διατηρείτε τουλάχιστον **3 αντίγραφα** των δεδομένων σας: το πρωτότυπο και 2 αντίγραφα ασφαλείας.

2 Διαφορετικά μέσα

Αποθηκεύστε τα αντίγραφα σε **2 διαφορετικά είδη μέσων**, π.χ. τοπικός δίσκος και NAS ή cloud.

1 εκτός εγκαταστάσεων

Τουλάχιστον **1 αντίγραφο αποθηκευμένο εκτός των εγκαταστάσεών σας** — σε cloud ή εξωτερική τοποθεσία.

Ο κανόνας 3-2-1-1-0

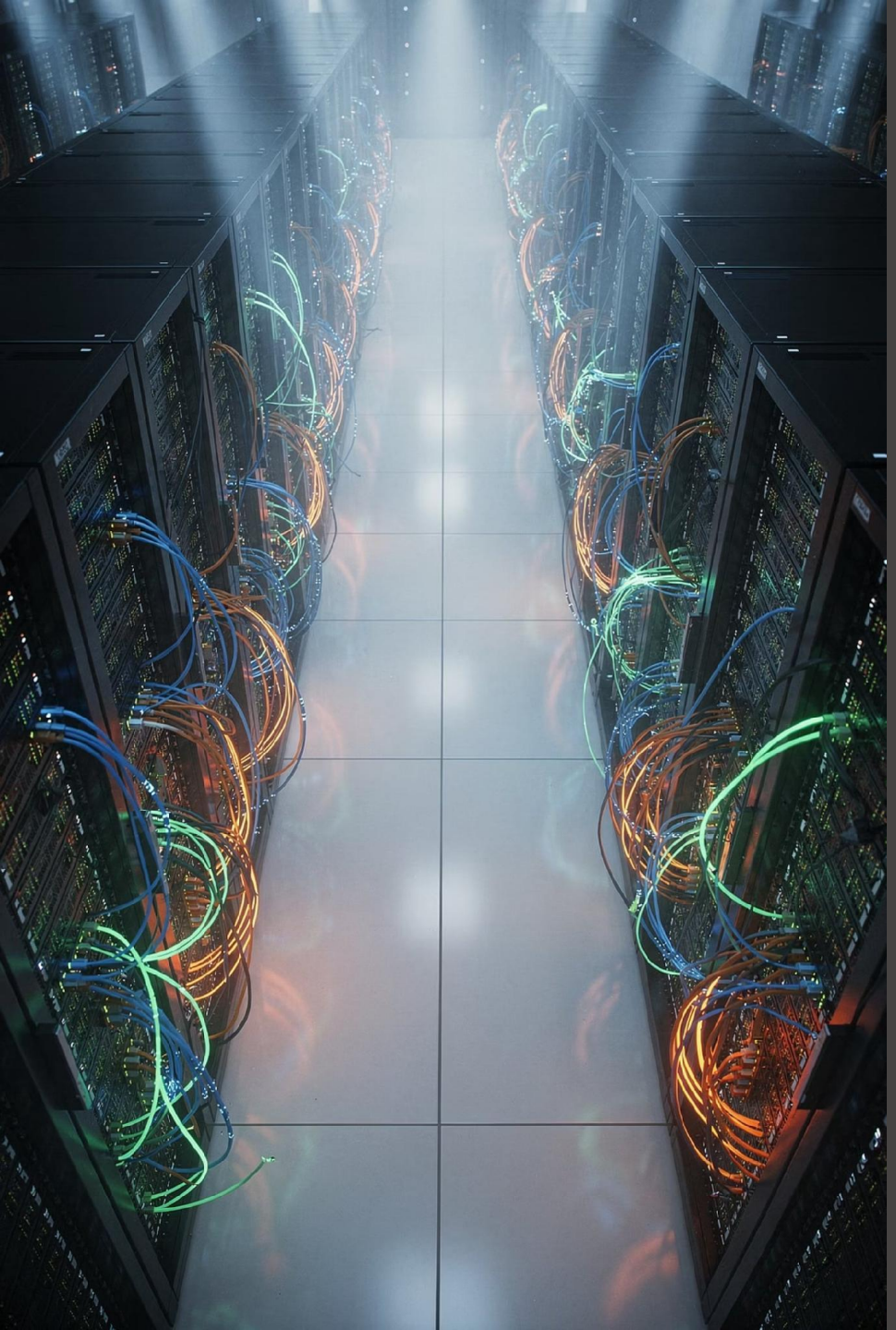
Η εξέλιξη του κλασικού κανόνα 3-2-1, σχεδιασμένη για την εποχή του ransomware. Προσθέτει δύο κρίσιμες απαιτήσεις για μέγιστη προστασία.

1	**3 αντίγραφα** Τρία σύνολα δεδομένων — πρωτότυπο και 2 αντίγραφα ασφαλείας.
2	**2 διαφορετικά μέσα** Αποθήκευση σε δύο ανεξάρτητα είδη μέσων αποθήκευσης.
3	**1 εκτός εγκαταστάσεων** Ένα αντίγραφο σε απομακρυσμένη τοποθεσία ή cloud.
4	**1 immutable ή offline** **Το κρίσιμο νέο στοιχείο:** Ένα αντίγραφο αμετάβλητο (immutable) ή εντελώς αποσυνδεδεμένο (air-gapped), απρόσιτο σε ransomware.
5	**0 σφάλματα** Τακτικός έλεγχος ακεραιότητας και επαλήθευση επαναφοράς — κανένα αντίγραφο δεν θεωρείται αξιόπιστο χωρίς επιτυχή restore test.

Τύποι backup

Η επιλογή του σωστού τύπου backup επηρεάζει άμεσα τον χρόνο δημιουργίας, τον αποθηκευτικό χώρο και την ταχύτητα ανάκτησης. Κάθε τύπος έχει διαφορετική χρήση.

Η πιο συχνή στρατηγική είναι ο **συνδυασμός Full + Incremental**: πλήρες backup εβδομαδιαίως και incremental καθημερινά για βέλτιστη ισορροπία μεταξύ ταχύτητας και αποθηκευτικού χώρου.



Cloud backup

Το cloud backup παρέχει ευελιξία, αυτόματη κλιμάκωση και γεωγραφική διασπορά δεδομένων. Ωστόσο, απαιτεί προσεκτική αξιολόγηση πριν την υιοθέτηση.

✅ Πλεονεκτήματα

- Αυτόματη γεωγραφική πλεονασμός δεδομένων
- Κλιμακούμενος αποθηκευτικός χώρος
- Χωρίς ανάγκη φυσικής υποδομής
- Εύκολη πρόσβαση από οπουδήποτε
- Υποστήριξη versioning και retention policies

⚠️ Περιορισμοί

- Εξάρτηση από σύνδεση internet
- Κόστος αποθήκευσης μεγαλώνει με τα δεδομένα
- Αργή ανάκτηση μεγάλων όγκων δεδομένων
- Ζητήματα συμμόρφωσης GDPR και εδαφικότητας
- Ο provider δεν εγγυάται πάντα αποκατάσταση

Offline & immutable backup

Το **offline backup** (air-gapped) και το **immutable backup** αποτελούν την ισχυρότερη άμυνα ενάντια στο ransomware, καθώς είναι απρόσιτα από οποιοδήποτε λογισμικό ή επιτιθέμενο.

Offline (Air-Gapped) backup

Το αντίγραφο είναι φυσικά αποσυνδεδεμένο από το δίκτυο. Χρησιμοποιεί φυσικά μέσα (tape, external disk) που αποθηκεύονται εκτός εγκαταστάσεων. Κανένα ransomware δεν μπορεί να το κρυπτογραφήσει εξ αποστάσεως.

Immutable backup

Τα δεδομένα αποθηκεύονται με τεχνολογία **WORM (Write Once, Read Many)**. Μόλις εγγραφούν, δεν μπορούν να τροποποιηθούν ή διαγραφούν για καθορισμένο χρονικό διάστημα — ούτε από administrators.

Object lock

Σύγχρονες cloud πλατφόρμες (AWS S3, Azure Blob) προσφέρουν Object Lock για immutability. Ιδανικό για οργανισμούς που θέλουν cloud backup με εγγυημένη προστασία από ransomware.

⚠ Ένα backup που είναι συνδεδεμένο στο δίκτυο και προσβάσιμο από backup servers μπορεί να κρυπτογραφηθεί από ransomware μαζί με τα πρωτότυπα δεδομένα.

Microsoft 365 backup

Η Microsoft **δεν εγγυάται αποκατάσταση δεδομένων** από τυχαία διαγραφή, ransomware ή κακόβουλη ενέργεια. Η ευθύνη του backup ανήκει στον οργανισμό (Shared Responsibility Model).

Exchange / Email

Backup mailboxes, deleted items retention έως 93 ημέρες — αλλά μόνο με επιπλέον ρυθμίσεις. Χρειάζεται 3rd-party λύση για πλήρη προστασία.

OneDrive

Versioning και Recycle Bin παρέχουν περιορισμένη προστασία. Δεν υποκαθιστούν backup σε περίπτωση μαζικής διαγραφής ή ransomware.

SharePoint

Η ανάκτηση περιορίζεται σε 93 ημέρες. Διαγραφέντα site collections χάνονται μόνιμα χωρίς εξωτερικό backup.

Microsoft Teams

Τα δεδομένα Teams αποθηκεύονται σε SharePoint και Exchange. Χωρίς ξεχωριστό backup, η ανάκτηση μηνυμάτων και αρχείων είναι εξαιρετικά δύσκολη.

Google workspace backup

Όπως και η Microsoft, η Google ακολουθεί το **Shared Responsibility Model**. Προστατεύει την υποδομή της, αλλά δεν αναλαμβάνει αποκατάσταση δεδομένων χρηστών σε όλα τα σενάρια.

Gmail

Το Gmail διατηρεί διαγραμμένα email για 30 ημέρες. Μετά, δεν υπάρχει δυνατότητα ανάκτησης από Google χωρίς 3rd-party backup tool. Κρίσιμο για επιχειρήσεις που χρησιμοποιούν email ως αρχείο.

Google Drive

Versioning διατηρείται για 30 ημέρες ή 100 εκδόσεις. Σε περίπτωση ransomware που επηρεάζει συγχρονισμένα αρχεία, η αποκατάσταση είναι χρονοβόρα και ατελής χωρίς εξωτερική λύση backup.

Google Calendar & Contacts

Συχνά παραβλέπονται, αλλά η απώλεια ημερολογίων και επαφών μπορεί να έχει σημαντικό αντίκτυπο στη λειτουργία της επιχείρησης. Απαιτείται εξωτερικό backup για πλήρη κάλυψη.

NAS και τοπικά backups

Τα NAS (Network Attached Storage) συστήματα είναι εξαιρετικά εργαλεία αποθήκευσης — αλλά συχνά παρεξηγούνται ως λύση backup. Κρίσιμη διαφορά: **RAID ≠ Backup**.

Τι κάνει το RAID

Το RAID παρέχει **πλεονασμό δίσκων** για προστασία από υλικό βλάβη. Αν ένας δίσκος αποτύχει, το σύστημα συνεχίζει να λειτουργεί. Δεν αντιγράφει δεδομένα σε διαφορετικές χρονικές στιγμές.

Τι ΔΕΝ κάνει το RAID

Το RAID **δεν προστατεύει** από ransomware (κρυπτογραφεί και τους δύο δίσκους), κατά λάθος διαγραφές, φυσικές καταστροφές (πυρκαγιά, πλημμύρα) ή κλοπή του NAS.

Σωστή χρήση NAS

Χρησιμοποιήστε το NAS ως **ένα από τα τρία αντίγραφα** στον κανόνα 3-2-1 — όχι ως τη μοναδική λύση backup. Συνδυάστε με cloud backup για πλήρη κάλυψη.

Προστασία του backup server

Ο backup server είναι ο πιο πολύτιμος στόχος για έναν επιτιθέμενο. Εάν καταληφθεί, καταστρέφεται η τελευταία γραμμή άμυνας. **Χρειάζεται ίδιο επίπεδο προστασίας με τα πιο κρίσιμα συστήματα.**

Multi-Factor Authentication (MFA)

Υποχρεωτικό MFA για όλη την πρόσβαση στον backup server και την κονσόλα διαχείρισης. Ακόμα και διαρροή κωδικού δεν αρκεί για πρόσβαση.

Least privilege access

Κάθε λογαριασμός έχει πρόσβαση μόνο στα δεδομένα που χρειάζεται. Κανένας χρήστης δεν έχει πρόσβαση σε όλα τα backups.

Διαχωρισμός λογαριασμών

Οι λογαριασμοί διαχείρισης backup να είναι **εντελώς ξεχωριστοί** από τους λογαριασμούς domain admin. Αποτρέπει lateral movement σε περίπτωση παραβίασης.

Κρυπτογράφηση αντιγράφων ασφαλείας

Η κρυπτογράφηση των backups δεν είναι προαιρετική — είναι απαίτηση GDPR και βέλτιστη πρακτική ασφάλειας. Προστατεύει τα δεδομένα τόσο κατά την αποθήκευση όσο και κατά τη μεταφορά.

Encryption at rest

Τα αποθηκευμένα δεδομένα κρυπτογραφούνται στα μέσα αποθήκευσης. Ακόμα και αν κλαπεί ο δίσκος, τα δεδομένα είναι αναγνώσιμα μόνο με το κλειδί αποκρυπτογράφησης. Χρησιμοποιήστε AES-256.

Encryption in transit

Κατά τη μεταφορά δεδομένων στο cloud ή σε εξωτερικά συστήματα, χρησιμοποιήστε TLS 1.2/1.3. Αποτρέπει υποκλοπή κατά τη μεταφορά μέσω δικτύου.

Διαχείριση κλειδιών

Τα κλειδιά κρυπτογράφησης πρέπει να αποθηκεύονται **ξεχωριστά** από τα δεδομένα — σε HSM ή εξωτερικό key management σύστημα. Απώλεια κλειδιού = μόνιμη απώλεια δεδομένων.

Αυτοματοποιημένα backups

Τα χειροκίνητα backups αποτυγχάνουν — λόγω ανθρώπινης αμέλειας, ξεχνιέτε, ή απλώς δεν εκτελούνται. **Η αυτοματοποίηση εξαλείφει τον ανθρώπινο παράγοντα** και εξασφαλίζει συνέπεια.

Προγραμματισμός

- Καθημερινό incremental backup (π.χ. 02:00)
- Εβδομαδιαίο full backup (Κυριακή)
- Μηνιαίο αρχειακό backup σε offline media
- Ορισμός retention policy ανά τύπο δεδομένων

Παρακολούθηση & ειδοποιήσεις

- Email/SMS ειδοποιήσεις για αποτυχίες
- Dashboard παρακολούθησης κατάστασης
- Αναφορές επιτυχίας/αποτυχίας ανά εργασία
- Έλεγχος διαθέσιμου χώρου αποθήκευσης
- SLA reporting και audit logs

Μια αποτυχημένη εργασία backup που δεν παρακολουθείται είναι εξίσου επικίνδυνη με την έλλειψη backup.

Έλεγχος επαναφοράς (Restore Testing)

Ένα backup που δεν έχει δοκιμαστεί για επαναφορά δεν είναι αξιόπιστο backup. Η ακεραιότητα και η ανακτησιμότητα των δεδομένων πρέπει να επαληθεύεται τακτικά.

1

Εβδομαδιαίος έλεγχος

Δοκιμή επαναφοράς τυχαίων αρχείων και επαλήθευση ακεραιότητας με hash comparison.

2

Μηνιαίος έλεγχος

Πλήρης restore δοκιμή κρίσιμων εφαρμογών σε απομονωμένο περιβάλλον (sandbox).

3

Τριμηνιαίος έλεγχος

Πλήρης DR drill: προσομοίωση καταστροφής και αποκατάσταση πλήρους περιβάλλοντος από μηδέν.

4

Τεκμηρίωση

Καταγραφή αποτελεσμάτων, χρόνου ανάκτησης και τυχόν προβλημάτων σε audit log.

RPO και RTO

Δύο από τις πιο κρίσιμες έννοιες στον σχεδιασμό backup και disaster recovery. Ορίζουν τι επίπεδο απώλειας και καθυστέρησης είναι αποδεκτό για τον οργανισμό.

RPO — Recovery Point Objective

«Πόσα δεδομένα μπορούμε να χάσουμε;»

Ορίζει το μέγιστο χρονικό διάστημα απώλειας δεδομένων που είναι αποδεκτό. Αν το RPO είναι 4 ώρες, χρειάζεστε backup κάθε 4 ώρες. Χαμηλό RPO = υψηλότερο κόστος.

RTO — Recovery Time Objective

«Πόσο γρήγορα πρέπει να επανέλθουμε;»

Ορίζει τον μέγιστο χρόνο αποκατάστασης μετά από περιστατικό. Αν το RTO είναι 2 ώρες, τα συστήματα πρέπει να είναι λειτουργικά σε 2 ώρες. Χαμηλό RTO = ανάγκη για hot standby συστήματα.

4h	8h	15'
Τυπικό RPO SMB	Τυπικό RTO SMB	RTO Επιχειρήσεων
Μέση αποδεκτή απώλεια δεδομένων για μικρές επιχειρήσεις	Μέσος αποδεκτός χρόνος αποκατάστασης	Στόχος για κρίσιμες επιχειρηματικές εφαρμογές

Διαχείριση περιστατικού ransomware

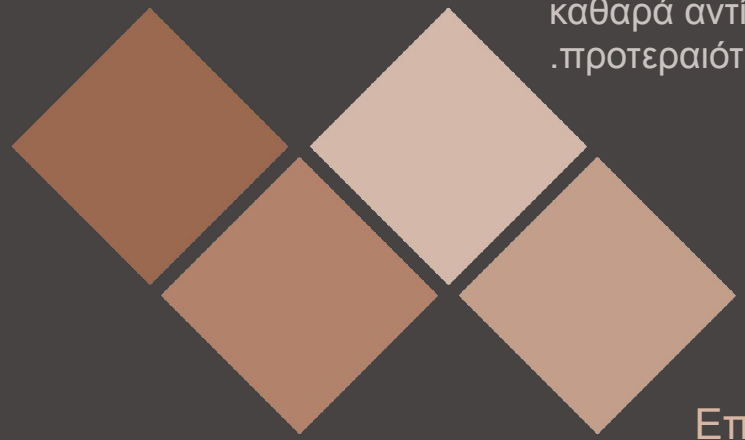
Σε περίπτωση επίθεσης ransomware, κάθε λεπτό μετράει. Η ύπαρξη προκαθορισμένου σχεδίου αντίδρασης μπορεί να κάνει τη διαφορά μεταξύ ανάκτησης σε ώρες ή εβδομάδες.

Αξιολόγηση

Καθορισμός εύρους και έλεγχος αντιγράφων .ασφαλείας

Αποκατάσταση

Επαναφορά από καθαρά αντίγραφα, .προτεραιότητα κρίσιμων



Απομόνωση

Αποσύνδεση μολυσμένων .συστημάτων αμέσως

Επικοινωνία

Ενημέρωση ενδιαφερομένων, .νομικών και αρχών

⚡ Άμεσες ενέργειες (0-1 ώρα)

Αποσύνδεση μολυσμένων συστημάτων, ενεργοποίηση IR team, τεκμηρίωση του περιστατικού. Μην πληρώσετε λύτρα χωρίς νομική συμβουλή.

🔍 Ανάλυση (1-4 ώρες)

Εντοπισμός του infection vector, ανίχνευση extent της ζημιάς, επαλήθευση ακεραιότητας backups πριν την αποκατάσταση.

🔄 Αποκατάσταση (4+ ώρες)

Restore από καθαρό backup, επαλήθευση συστημάτων, σταδιακή επαναφορά λειτουργιών βάσει DRP.

Case study 1: επίθεση ransomware χωρίς backup

Μια μεσαία ελληνική εταιρεία παροχής υπηρεσιών (50 υπάλληλοι) δέχτηκε επίθεση ransomware μέσω phishing email. Το malware κρυπτογράφησε **όλα τα αρχεία**, συμπεριλαμβανομένων των "backups" που βρίσκονταν σε συνδεδεμένο δίσκο.

Λάθη που έγιναν

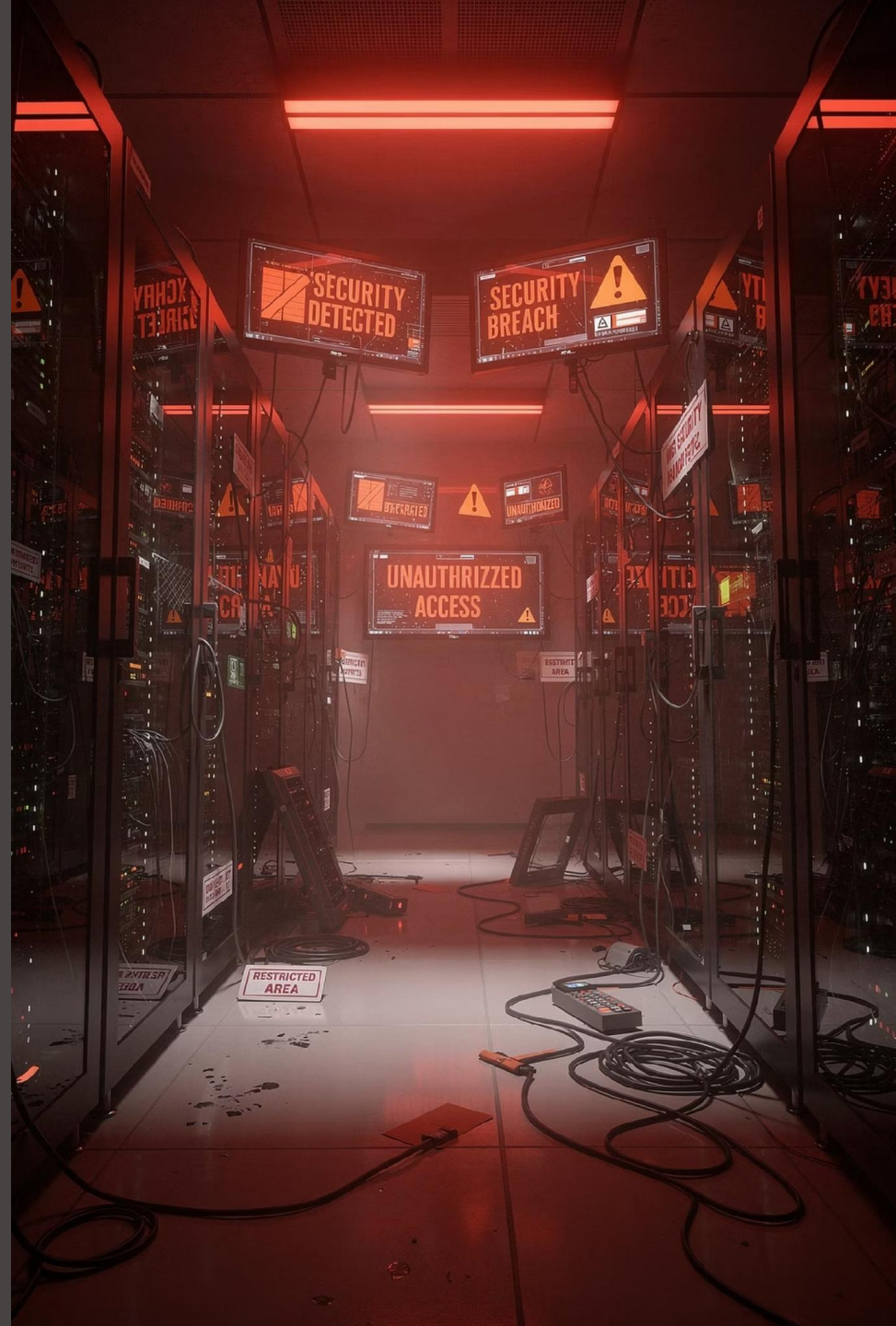
- Backup μόνο σε συνδεδεμένο USB δίσκο
- Δεν υπήρχε offline ή cloud αντίγραφο
- Δεν είχε γίνει ποτέ restore test
- Απουσία MFA στους backup λογαριασμούς

Συνέπειες

- 3 εβδομάδες διακοπή λειτουργίας
- Πληρωμή λύτρων €45.000
- Απώλεια δεδομένων 6 μηνών
- Μόνιμη ζημιά στη φήμη και απώλεια πελατών

Τι έπρεπε να γίνει

- Κανόνας 3-2-1 με cloud backup
- Immutable backup για κρίσιμα δεδομένα
- Τακτικά restore tests
- Εκπαίδευση προσωπικού σε phishing



Case study 2: Επιτυχής ανάκαμψη με immutable backup

Εταιρεία logistics με 200 υπαλλήλους δέχτηκε επίθεση ransomware που κρυπτογράφησε servers παραγωγής και primary backups. Χάρη σε immutable cloud backup, η αποκατάσταση ήταν πλήρης.

Η σωστή προετοιμασία

- Immutable backup σε cloud (AWS S3 Object Lock)
- Μηνιαία DR drills με documented procedures
- Ξεχωριστοί λογαριασμοί backup με MFA
- Καθορισμένο RTO 4 ωρών για κρίσιμα συστήματα

Αποτέλεσμα αντίδρασης

- **Χρόνος ανάκτησης: 3,5 ώρες**
- Απώλεια δεδομένων: μόλις 2 ώρες (RPO)
- Μηδενική πληρωμή λύτρων
- Ελάχιστος αντίκτυπος στη λειτουργία

Η επένδυση σε immutable backup και τακτικές δοκιμές εξοικονόμησε εκατοντάδες χιλιάδες ευρώ σε λύτρα, downtime και νομικές υποχρεώσεις.

Συνηθισμένα λάθη στα backups

Η πλειονότητα των αποτυχιών backup οφείλεται σε γνωστά και αποτρέψιμα λάθη. Αναγνωρίστε τα και διορθώστε τα πριν γίνουν κρίση.

→ Backups στον ίδιο δίσκο/server

Αν το πρωτότυπο και το backup βρίσκονται στο ίδιο φυσικό μέσο ή server, μια βλάβη ή ransomware τα καταστρέφει και τα δύο ταυτόχρονα.

→ Ποτέ δεν ελέγχεται η επαναφορά

Πολλοί οργανισμοί ανακαλύπτουν ότι τα backups τους είναι κατεστραμμένα ή ελλιπή μόνο όταν τα χρειαστούν επειγόντως.

→ Εξαίρεση κρίσιμων δεδομένων

Βάσεις δεδομένων που είναι ανοιχτές κατά το backup, αρχεία configuration, email αρχεία — συχνά λείπουν από τη λίστα backup.

→ Παλιές ή ξεπερασμένες πολιτικές

Η στρατηγική backup δεν ενημερώνεται καθώς μεγαλώνει η επιχείρηση, προστίθενται νέα συστήματα ή αλλάζουν οι απαιτήσεις.

→ Ανεπαρκής παρακολούθηση

Αποτυχημένες εργασίες backup που δεν εντοπίζονται για ημέρες ή εβδομάδες αφήνουν τον οργανισμό χωρίς προστασία.

Βέλτιστες πρακτικές backup

Μια ολοκληρωμένη στρατηγική backup συνδυάζει τεχνολογία, διαδικασίες και ανθρώπους. Εφαρμόστε αυτές τις πρακτικές για μέγιστη προστασία.

Κρυπτογράφηση

AES-256 encryption at rest και TLS in transit. Ξεχωριστή αποθήκευση κλειδιών. Υποχρεωτικό για GDPR compliance.

MFA παντού

Multi-factor authentication για όλη την πρόσβαση backup συστημάτων. Ξεχωριστοί λογαριασμοί backup χωρίς domain admin δικαιώματα.

Offline αντίγραφα

Τουλάχιστον ένα αντίγραφο εντελώς αποσυνδεδεμένο (air-gapped) ή immutable. Απαραίτητο για προστασία από ransomware.

Τεκμηρίωση & εκπαίδευση

Γραπτές διαδικασίες restore, τακτική εκπαίδευση IT team, ετήσιες DR ασκήσεις. Η τεχνολογία χωρίς γνώση αποτυγχάνει.

Checklist: 20 σημεία ελέγχου για επιχειρήσεις

Χρησιμοποιήστε αυτή τη λίστα για να αξιολογήσετε την τρέχουσα κατάσταση της στρατηγικής backup της επιχείρησής σας.

📋 Στρατηγική & πολιτική

- ☐ Καθορισμένα RPO και RTO για κάθε σύστημα
- ☐ Τεκμηριωμένη πολιτική backup
- ☐ Εφαρμογή κανόνα 3-2-1 ή 3-2-1-1-0
- ☐ Κάλυψη όλων των κρίσιμων δεδομένων
- ☐ Retention policy ανά τύπο δεδομένων

🔒 Ασφάλεια

- ☐ MFA σε όλους τους backup λογαριασμούς
- ☐ Κρυπτογράφηση at rest και in transit
- ☐ Ξεχωριστοί λογαριασμοί backup (least privilege)
- ☐ Τουλάχιστον ένα immutable ή offline αντίγραφο
- ☐ Εξωτερική αποθήκευση κλειδιών κρυπτογράφησης

⚙️ Λειτουργία & αυτοματοποίηση

- ☐ Πλήρης αυτοματοποίηση εργασιών backup
- ☐ Ειδοποιήσεις για αποτυχημένες εργασίες
- ☐ Παρακολούθηση διαθέσιμου αποθηκευτικού χώρου
- ☐ Backup Microsoft 365 / Google Workspace
- ☐ Κάλυψη NAS με εξωτερικό backup (όχι μόνο RAID)

✅ Δοκιμές & αναθεώρηση

- ☐ Εβδομαδιαίος έλεγχος ακεραιότητας αρχείων
- ☐ Μηνιαίο restore test κρίσιμων εφαρμογών
- ☐ Ετήσια πλήρης DR άσκηση (disaster recovery drill)
- ☐ Τεκμηρίωση αποτελεσμάτων ελέγχων
- ☐ Ετήσια αναθεώρηση και ενημέρωση πολιτικής

Συμπεράσματα: τα backups ως τελευταία γραμμή άμυνας

Κανένα σύστημα ασφάλειας δεν είναι αλάνθαστο. Firewalls, antivirus και EDR μειώνουν τον κίνδυνο — αλλά τα **αντίγραφα ασφαλείας εγγυώνται την επιβίωση** όταν όλα τα άλλα αποτύχουν.

Σχεδιάστε σωστά

Εφαρμόστε κανόνα 3-2-1-1-0, ορίστε RPO/RTO, τεκμηριώστε τις διαδικασίες σας.

Αυτοματοποιήστε

Εξαλείψτε τον ανθρώπινο παράγοντα. Παρακολουθήστε κάθε εργασία backup και αντιδράτε άμεσα σε αποτυχίες.

Δοκιμάστε τακτικά

Ένα backup χωρίς restore test δεν είναι backup. Επαληθεύστε τακτικά ότι μπορείτε να ανακτήσετε ό,τι χρειάζεστε.

> «Υπάρχουν δύο τύποι οργανισμών: αυτοί που έχουν χάσει δεδομένα και αυτοί που δεν το ξέρουν ακόμα. Η διαφορά είναι ένα καλό backup.»