



General Data Protection Regulation

GDPR – Riforma europea delle regole per la protezione dei dati



Il 25 maggio 2018 entrerà in vigore il Regolamento Generale sulla Protezione dei Dati e definirà norme uniche per tutti i trattamenti dei dati personali effettuati nei Paesi dell'Unione Europea.

Ragion per cui bisogna farsi trovare preparati davanti alla legge e alle sfide del mercato! Questa riforma coinvolge direttamente aziende sia dentro che fuori l'Europa e pubbliche amministrazioni, la mancata conformità a queste disposizioni potrà comportare ammende che possono arrivare fino a 20 milioni di euro o al 4% del fatturato annuo.

OmniNet, grazie a un'esperienza pluriennale nel settore della sicurezza e dei servizi gestiti, è in grado di offrirti le migliori soluzioni "As a Service" per dare un riscontro al tema della "Gestione del Rischio" presente nel GDPR, nelle sue varie sfaccettature. La prima cosa da fare è (e non è banale) conoscere l'esatta articolazione e configurazione della propria Infrastruttura informatica, mappando tutti gli asset che la compongono e valutandone il relativo livello di rischio.

ANALISI DI BASE

NETWORK ASSESSMENTS

Una valutazione IT ideale per generare una serie di informazioni utili su tutto ciò che è connesso alla rete (fisico e virtuale), oltre alla condizione generale dell'infrastruttura. Vengono evidenziate eventuali discrepanze e/o violazioni con la Policy aziendale di sicurezza.

SECURITY ASSESSMENTS

Aggiunge un'altra dimensione agli assessment di rete, includendo vulnerabilità esterne, comportamenti dell'utente, autorizzazioni, login, vulnerabilità interne di rilievo e molto altro. Un check sistematico per tenere sotto controllo la rete aziendale.

ANALISI OPZIONALI

SQL SERVER ASSESSMENTS

Opzionalmente è possibile avere anche un SQL Server Assessment, per completare l'insieme con ulteriori report destinati a chiunque sia responsabile del mantenimento di SQL Server, inclusi DBA.

REPORT della Network Assessment

- ✓ Client Risk Report: Report con rappresentazione della vista ad alto livello generale della vostra rete, con chiare indicazioni dove siano riscontrati problemi. Ogni area di problemi include la descrizione con la relativa raccomandazione per la risoluzione.
- ✓ Full Network Assessment Report: il processo di scansione estrae centinaia di pagine di dati relative alla configurazione e all'attività di una rete.
- ✓ Network Site Diagram: una volta lanciata una scansione, è possibile generare un diagramma che elenca e categorizza tutti gli asset disponibili sulla rete.
- ✓ Asset Detail Report: fornisce informazioni dettagliate circa tutti i singoli asset rilevati per ciascuna scansione di rete.
- ✓ Network Comparison Assessment Report: confronta i risultati di due scansioni qualsiasi evidenziando i cambiamenti intervenuti nel frattempo.
- ✓ Excel Analysis Export/Report: il software offre la possibilità di esportare tutti gli asset e tutte le configurazioni risultanti da una scansione in formato di file Excel.
- ✓ External Vulnerabilities Summary: per ciascun indirizzo IP viene fornito un riepilogo di tutte le vulnerabilità di sicurezza e di tutti gli allarmi generati dal sistema.
- ✓ Migration Readiness Report: determina le macchine Windows che devono essere aggiornate, se richiedono aggiornamenti hardware o se devono essere sostituite.

REPORT della Security Assessment

- ✓ Network Security Risk Review: comprende un punteggio Security Risk Score proprietario e un grafico che mostra lo stato di salute relativo della sicurezza di rete e mostra un riepilogo del numero di computer interessati da problemi.
- ✓ External Vulnerabilities Full Detail Report: identifica vulnerabilità di sicurezza, allarmi e altre informazioni in materia di sicurezza della rete oltre a una scansione NMap completa che controlla tutte le porte segnalando quelle aperte.
- ✓ Outbound Security Report: evidenzia la deviazione dagli standard di settore in termini di accessibilità di protocolli e porte in uscita, comprende nell'analisi anche le reti wireless disponibili e fornisce informazioni sull'accessibilità dei contenuti internet.
- ✓ Security Policy Assessment Report: effettua una verifica dettagliata delle policy di sicurezza in vigore sia nell'intero dominio sia localmente sulle macchine.
- ✓ Share Permission Report: fornisce un elenco completo di tutte le condivisioni di rete ordinate per computer con l'indicazione di quali utenti e gruppi hanno accesso a quali dispositivi e file, e a quale livello.
- ✓ User Permissions Report: fornisce una panoramica sui permessi in base agli utenti e mostra tutti i computer e i file condivisi ai quali hanno accesso.
- ✓ User Behavior Analysis Report: mostra tutti i login completati e falliti di ciascun utente.
- ✓ Login Failures by Computer Report: mostra tutti i login completati e falliti raggruppati a seconda del computer.
- ✓ Login History by Computer Report: identifica gli utenti che hanno eseguito il login su un'altra macchina.
- ✓ Security Risk Assessment - Dark Web ID: segnala se i dati e le credenziali sono stati esposti tramite il dark web pericolosamente. La conoscenza di queste esposizioni consente di evitare le violazioni che sono tipicamente generate dalle malevole attività web.

REPORT della SQL Server Assessment

- ✓ Routine Health Report: valuta lo stato di salute di SQL Server usando tre categorie principali: parametri di configurazione, file e risorse.
- ✓ SQL Server Detail Report: fornisce un dettaglio dei parametri di configurazione e lo stato di salute complessivo di SQL Server analizzando anche prestazioni e backup.
- ✓ Database Detail Report: fornisce un dettaglio dei parametri di configurazione e lo stato di salute dei singoli database residenti su SQL Server.
- ✓ Maintenance Plan Report: mostra tutti i piani e sotto-piani di manutenzione che eseguono attività di routine su SQL Server.
- ✓ SQL Server Agent Jobs Report: identifica tutti i job (attivi e inattivi) dell'agente SQL Server.

- Data-Collector non invasivi: nessun software da installare, nessun agente. Saranno eseguiti tool direttamente sul Domain Controller e/o su qualunque altro computer di rete, inserendo credenziali amministrative e lasciando che il sistema faccia tutto il lavoro.
- Scansioni programmate: si può automatizzare la raccolta di dati ad intervalli regolari (opzionale)
- Scansioni off-network: un tool di scansione separato da utilizzare sui computer non collegati alla rete. Permette di consolidare i dati dei computer off-network all'interno dei report principali
- Sicuro: nessuna informazione business né password viene raccolta o trasmessa e non occorre modificare le impostazioni del firewall
- Raccolta dati da ambienti Windows, Mac e Linux