mobisec

GUIDA ALLA NIS2

COME CAMBIANO LE PRIORITÀ NELLA GESTIONE DELLA SICUREZZA PER LE AZIENDE CHE HANNO UN'APPLICAZIONE MOBILE

mobisec.com

mobisec

I NOSTRI 8 PUNTI

MENU

VOTATI ALLA SECURITY

SU DI NOI

Fondata nel 2015, Mobisec si è occupata fin dal principio di **cybersecurity applicativa,** nella consapevolezza che la responsabiltà relativa alla sicurezza infrastrutturale passa sempre di più nelle mani di hyperscaler e cloud service provider; ciò rende i datacenter e il network particolarmente resilienti, mentre lascia fortemente esposto il mondo logico-applicativo.

Siamo nati proprio per rispondere alle esigenze di sicurezza di un mondo sempre più connesso, sviluppando competenze e conoscenze uniche in ethical hacking e innovazione. Offriamo soluzioni su misura per fornire sicurezza e serenità a chi gestisce in azienda la cybersecurity degli applicativi, dei dispositivi mobili e dell'IoT.

VOTATI ALLA SECURITY

SU DI NOI

Nel 2024 siamo diventati, unica azienda italiana tra le 20 presenti a livello mondiale, **membri ufficiali dell'ADA** (App Defense Alliance), l'organismo della Linux Foundation che ha come steering committee Microsoft, Google, Meta e che ha la missione di garantire la sicurezza e la privacy dell'ecosistema delle app definendo i framework di riferimento per i test e i laboratori.

Siamo **stabilmente nel gruppo dei *contributor* dell'OWASP** (Open Worldwide Application Security Project), il massimo ente internazionale per la definizione degli standard e delle procedure di sicurezza nel mondo applicativo; nel 2024 contribuiremo in maniera diretta alla mappatura delle Weakness, la nuova categoria introdotta proprio dall'OWASP per le Mobile Application (MASWE).

Mobisec è inclusa tra le soluzioni di **Mobile Application Security Testing all'interno dei Gartner Peer Insights**, con una valutazione media di 4,5/5.

⭐⭐⭐⭐

Mobisec ha ottenuto la **certificazione ISO 27001:2022 per la gestione della sicurezza delle informazioni**, e segue gli standard della certificazione ISO 9001:2015 per i sistemi di gestione della qualità.

PREMESSE

NIS2

Cos'è - La NIS2 (Network and Information Security-2) è la direttiva entrata in vigore il 17 gennaio 2023 e che gli Stati Membri dell'Unione Europea **devono recepire entro il 17 ottobre 2024**; ha l'obiettivo di stabilire dei riferimenti comuni all'interno dell'Unione sui temi di sicurezza informatica e opera in maniera sinergica con altre normative, come il GDPR, il Cyber Resilience Act, la normativa DORA.

A chi si applica – Sebbene a prima vista possa sembrare applicabile solo a una ristretta base di aziende, considerate ad "alta criticità", di fatto si estende a tutta la supply chain, impattando quindi un numero molto più ampio di aziende.

Sicurezza delle Mobile Application – La normativa ricomprende un ampio ventaglio di requisiti che le aziende devono soddisfare per potersi considerare *compliant*, in questa guida ci concentriamo su quei punti che riguardano in maniera specifica la Mobile Application security.

1. COSA SI INTENDE PER SISTEMA INFORMATIVO?

CI SONO ANCHE LE APP

L'ARTICOLO

Art. 2 <<definizioni>>, comma 1, lettera E, «sistema informativo e di rete»:

1) una rete di comunicazione elettronica ai sensi dell'articolo 2, comma 1, lettera vv), del decreto legislativo 1° agosto 2003, n. 259;

2) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali;

3) i dati digitali conservati, elaborati, estratti o trasmessi per mezzo di reti o dispositivi di cui ai numeri 1) e 2), per il loro funzionamento, uso, protezione e manutenzione;

L'articolo mette in luce un punto cruciale: la sicurezza informatica non è più un optional, ma un imperativo categorico. Non si tratta solo di proteggere le infrastrutture e i software tradizionali, ma di estendere la sicurezza a tutto ciò che è connesso e che elabora dati digitali. Inclusi anche smartphone e le innumerevoli app che utilizziamo quotidianamente.

Ogni app che viene scaricata ed installata è come una porta o una finestra. Più ne hai, più devi essere sicuro che siano ben chiuse e protette. Ecco perché la NIS2 include anche questi dispositivi e le relative applicazioni.

In poche parole, l'articolo ci ricorda che viviamo in un mondo sempre più connesso e che la sicurezza deve essere una priorità, non solo per le grandi infrastrutture, ma anche per i dispositivi portatili.

2. GESTIONE DEI RISCHI

ANCHE NELL'AMBITO DELLE MOBILE APP

L'ARTICOLO

Art. 23 comma 1 <<obblighi di amministrazione e direttivi>>:

Gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e dei soggetti importanti:

a) approvano le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica adottate da tali soggetti ai sensi dell'articolo 24;

b) Sovrintendono all'implementazione degli obblighi di cui al presente capo e di cui all'articolo 7;

c) sono responsabili delle violazioni di cui al presente decreto.

Questo articolo mette in evidenza l'importanza del ruolo degli organi di amministrazione e direttivi nel garantire la sicurezza informatica. Non si tratta solo di approvare le misure di gestione dei rischi, ma anche di supervisionare la loro implementazione e di assumersi la responsabilità per eventuali violazioni, anche nell'ambito degli applicativi mobile.

L'approccio proattivo non si limita al mettere in atto misure di sicurezza, ma anche di monitorarle costantemente e di essere pronti a intervenire in caso di problemi. La sicurezza informatica richiede un impegno costante da parte di tutti, a partire dagli organi di amministrazione e direttivi.

3. SICUREZZA DELLA SUPPLY CHAIN

RESPONSABILITÀ PER SOFTWARE HOUSE E AZIENDA COMMITTENTE

L'ARTICOLO

Art. 3 comma 10 <<ambito di applicazione>>:

Il presente decreto si applica, infine, indipendentemente dalle sue dimensioni, all'impresa collegata ad un soggetto essenziale o importante, se soddisfa almeno uno dei seguenti criteri:

a) adotta decisioni o esercita una influenza dominante sulle decisioni relative alle misure di gestione del rischio per la sicurezza informatica di un soggetto importante o essenziale;

b) detiene o gestisce sistemi informativi e di rete da cui dipende la fornitura dei servizi del soggetto importante o essenziale;

c) effettua operazioni di sicurezza informatica del soggetto importante o essenziale;

d) fornisce servizi TIC o di sicurezza, anche gestiti, al soggetto importante o essenziale.

L'articolo 3, comma 10 della legge NIS2 amplia l'ambito di applicazione della sicurezza informatica, includendo non solo i soggetti essenziali o importanti, ma anche le imprese a essi collegate. Questo ha importanti implicazioni per la sicurezza delle applicazioni mobile.

Cosa significa? Che la sicurezza delle applicazioni mobile non è più solo una questione che riguarda i singoli sviluppatori o le aziende di sviluppo software. Ora, anche le aziende che commissionano lo sviluppo di queste applicazioni e le utilizzano per il proprio business devono assumersi la responsabilità della loro sicurezza.

Tutti gli attori coinvolti, dalle aziende di sviluppo alle aziende utilizzatrici, devono collaborare per garantire la sicurezza delle applicazioni mobile.

4. PROTEZIONE DEI DATI

SI RAFFORZA IL GDPR

L'ARTICOLO

Art. 3, comma 11 <<ambito applicazione>> :

Resta ferma la disciplina in materia di protezione dei dati personali di cui al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, e al decreto legislativo 30 giugno 2003, n. 196, nonché in materia di lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile di cui al decreto legislativo 4 marzo 2014, n. 39.

La protezione dei dati rimane prioritaria. La NIS2 non scavalca i regolamenti GDPR, ma li rafforza, sottolineando ulteriormente l'importanza di mantenere i dati protetti.

Sono sempre di più le applicazioni all'interno degli smartphone che veicolano e gestiscono frazioni importanti delle vite degli utenti. Nell'ottica di rendere standard la responsabilizzazione delle aziende che utilizzano le applicazioni per fare business, la NIS2 riporta l'attenzione sul tema dei dati personali.

Svolgere test specifici per analizzare la robustezza delle strutture è fondamentale per essere compliant rispetto a quanto richiesto dalle normative.

5. AGGIORNAMENTI E MANUTENZIONE

FONDAMENTALE MONITORARE I CICLI DI SVILUPPO E RILASCIO

L'ARTICOLO

Art. 24, comma 1, comma 2 lettera E <<Obblighi in materia di misure di gestione dei rischi per la sicurezza informatica>>:

I soggetti essenziali e i soggetti importanti adottano misure tecniche, operative e organizzative adeguate e proporzionate […] alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete […], nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi.

[...]

Le misure di cui al comma 1 sono basate su un approccio multi-rischio, volto a proteggere i sistemi informativi e di rete nonché il loro ambiente fisico da incidenti, e comprendono almeno i seguenti elementi:

[...] e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, ivi comprese la gestione e la divulgazione delle vulnerabilità;

La NIS 2 parla chiaro: è obbligatorio adottare tutte quelle misure che aggiornino, mantengano e si applichino per la corretta gestione della sicurezza dei sistemi informativi, ivi incluse le applicazioni mobile, e la corretta gestione delle vulnerabilità. Gli aggiornamenti devono essere rilasciati prontamente per risolvere le falle di sicurezza, questo è possibile solo attraverso una procedura di monitoraggio continuo delle vulnerabilità presenti nelle applicazioni ad ogni rilascio.

Questo aspetto è di fondamentale importanza per le applicazioni mobile, che una volta rilasciate di fatto sono fuori dal perimetro di controllo dell'azienda.

6. FORMAZIONE E CONSAPEVOLEZZA

INTERIORIZZARE LE BEST PRACTICE

L'ARTICOLO

Art. 23 comma 2, lettere A, B <<Organi di amministrazione e direttivi>> : *a) sono tenuti a seguire una formazione in materia di sicurezza informatica; b) promuovono l'offerta periodica di una formazione coerente a quella di cui alla lettera a) ai loro dipendenti, per favorire l'acquisizione di conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi per la sicurezza informatica e il loro impatto sulle attività del soggetto e sui servizi offerti.*

Questo articolo della NIS2 ci ricorda che la formazione sulla cybersecurity non è solo un dovere, ma un'opportunità.
Non si tratta solo di imparare a proteggere i dati o a prevenire gli attacchi.
Si tratta di capire come il mondo digitale funziona, come le applicazioni e i dispositivi mobili che usiamo ogni giorno possono essere progettati e sviluppati con la sicurezza in mente.
Immaginate corsi come "Security by Design" o "DevSecOps", dove si impara a programmare in modo sicuro fin dall'inizio, non come un'implementazione in fasi successive. E non dimentichiamo la formazione a livello manageriale, perché la sicurezza è una responsabilità di tutti.

Mentre l'articolo di legge potrebbe sembrare austero, pensate a questo come un invito ad esplorare, imparare e innovare. Dopotutto, la cybersecurity è un viaggio, non una destinazione. E che viaggio sarebbe senza un po' di apprendimento lungo la strada?

7. MONITORAGGIO E RISPOSTA AGLI INCIDENTI

PREVENIRE È MEGLIO CHE CURARE

L'ARTICOLO

Art. 35 comma 3 <<Monitoraggio, analisi e supporto>> :

L'Autorità nazionale competente NIS, ai fini dell'attività di monitoraggio di cui al comma 2, può:

a) richiedere ai soggetti una rendicontazione, anche periodica, ivi incluse autovalutazioni e piani di implementazione, dello stato di attuazione degli obblighi di cui al presente decreto, nonché le informazioni necessarie per lo svolgimento dei propri compiti istituzionali, dichiarando la finalità della richiesta; b) richiedere ai soggetti l'esecuzione, periodica o mirata, di audit sulla sicurezza, in particolare in caso di incidente significativo o di violazione del presente decreto da parte del soggetto;

c) richiedere ai soggetti l'esecuzione di scansioni di sicurezza basate su criteri di valutazione dei rischi obiettivi, non discriminatori, equi e trasparenti, se necessario in cooperazione con il soggetto interessato;

In questo articolo viene messa in risalto l'importanza di un monitoraggio continuo e accurato per rispondere agli incidenti di sicurezza, inclusi quelli che riguardano le applicazioni mobile. La sicurezza non può essere lasciata al caso: è fondamentale eseguire regolari pentesting ben fatti per individuare e correggere tempestivamente le vulnerabilità. La frequenza e la qualità di questi test sono essenziali per prevenire incidenti significativi. Se l'azienda non dispone delle competenze interne necessarie, è altrettanto fondamentale collaborare con partner esperti nel settore. La collaborazione con professionisti esterni garantisce che le scansioni di sicurezza siano basate su criteri di valutazione dei rischi obiettivi, non discriminatori, equi e trasparenti, come richiesto dalla normativa. Mantenere alta l'attenzione sulla sicurezza e rispondere rapidamente agli incidenti è cruciale non solo per proteggere i dati sensibili, ma anche per garantire la continuità operativa e la fiducia degli utenti.

8. COMPLIANCE E AUDIT

MONITORAGGIO COSTANTE

L'ARTICOLO

Art. 34 comma 7 <<Principi generali per lo svolgimento delle attività di vigilanza ed esecuzione>>

Gli audit sulla sicurezza, periodici e mirati, nonché le scansioni di sicurezza … sono svolti da organismi indipendenti (e si basano su valutazioni del rischio effettuate dall'Autorità nazionale competente NIS o dal soggetto sottoposto ad audit o su altre informazioni disponibili in relazione ai rischi.)

Art. 35 comma 3 par. b) <<Monitoraggio, analisi e supporto>>

L'Autorità nazionale competente NIS, ai fini dell'attività di monitoraggio … può: richiedere ai soggetti l'esecuzione, periodica o mirata, di audit sulla sicurezza, in particolare in caso di incidente significativo o di violazione del presente decreto da parte del soggetto.

Gli articoli 34 e 35 della normativa di recepimento del NIS2 sottolineano l'importanza cruciale di una sicurezza informatica a 360 gradi. Non basta avere un'infrastruttura robusta e software aggiornati: le organizzazioni devono anche garantire che anche le applicazioni rispettino le normative vigenti. L'Autorità nazionale competente NIS gioca un ruolo chiave in questo processo, richiedendo audit di sicurezza periodici, specialmente in caso di incidenti significativi o violazioni delle normative. Adottare un approccio proattivo non solo aiuta a prevenire potenziali minacce, ma garantisce anche che le organizzazioni rimangano sempre un passo avanti rispetto ai rischi emergenti. In definitiva, questi articoli non sono solo un obbligo, ma una guida preziosa per mantenere al sicuro il cuore pulsante del business. La conformità alle normative non deve essere vista come un peso, ma come un'opportunità per rafforzare la resilienza informatica e proteggere il business nel lungo termine.

mobisec

CONCLUSIONI

MOBISEC PER LA NIS2

Le implicazioni della NIS2 sulla *mobile application security* obbligano a una riorganizzazione delle agende di chi ha la responsabilità della sicurezza dell'azienda; sono temi che non possono essere ignorati e per i quali Mobisec offre un valido supporto volto a raggiungere la conformità con una combinazione di servizi chiave: effettuiamo valutazioni di sicurezza per le tue applicazioni mobili, aiutandoti ad affrontare i punti deboli prima che diventino un vero problema di compliance. Attraverso **Vulnerability Assessment e Pentesting documentati da report con indicazioni mirate su come mitigare le criticità rilevate**, ti aiutiamo a rispettare gli standard di sicurezza più rigorosi, rafforzando allo stesso tempo le competenze interne della tua azienda in materia di *mobile application security*.

mobisec

staysafe@mobisec.com

Mobisec

Viale della Repubblica 22/III
Villorba (TV)

4010 Moorpark Ave
San Jose, CA 95117

mobisec.com

RESTIAMO IN CONTATTO.