Sicurezza WordPress

controllare il sito e gestire un attacco

Che cosa verificare, quali prove chiedere, che cosa fare se è violato

1 Il controllo non riguarda solo WordPress



Esempio: WordPress è aggiornato, ma…

il pannello hosting usa una password condivisa → **viene compromessa** l'email che permette di recuperarla → **l'attaccante prova a** entrare senza passare **da WordPress**

Un fornitore cessato? Verifica i suoi accessi ovunque
su tutti i servizi coinvolti, non soltanto dentro WordPress

2 Le prove da chiedere al gestore

Non dimostra nulla	La prova che serve
la pagina iniziale si apre dopo l'aggiornamento	una richiesta con allegato arriva al destinatario, sul sito pubblico
la notifica «backup completato»	un ripristino in prova, con data, esito e verifica delle funzioni
il lucchetto HTTPS nel browser	riguarda la connessione: plugin, account e copie vanno controllati a parte
una password condivisa, da cambiare a tutti quando qualcuno esce	account personali con doppia verifica: si revoca solo quello di chi esce

Prova mancante = controllo non dimostrato
non significa che il sito sia già compromesso

3 Se il sito è stato violato: cinque passi

1. **Annota i segnali**
   avviso, pagine coinvolte, ora della scoperta, modifiche recenti
2. **Contieni il danno e conserva le prove**
   log e copia protetta prima delle operazioni che cancellano
3. **Recupera gli accessi e correggi la causa**
   un backup può già contenere l'infezione
4. **Verifica il ritorno al servizio**
   pagine, moduli, allegati, notifiche e collegamenti
5. **Documenta causa e interventi**
   e concorda i controlli contro eventuali ricomparse

72 ore
dati personali: quando la notifica è dovuta, senza ingiustificato ritardo e, ove possibile, entro 72 ore

giorni o settimane
il riesame di sicurezza di Google dopo la correzione: da alcuni giorni a qualche settimana

Il sito di nuovo online non chiude l'incidente
la rimozione dell'avviso di Google è una verifica separata

Fonte: WordPress, Google Search Console, Garante privacy; esempi dell'articolo

KLC www.klc.it

Fonte: KLC · Checklist sicurezza WordPress: come controllare il sito e gestire un attacco
https://www.klc.it/blog/siti-web/checklist-sicurezza-wordpress-e-incident-response/