Ciclo webinar SICUREZZA INFORMATICA - **RISPOSTE degli esperti alle domande inevase nel corso del webinar del** 11.11.2021

AMATO

1. **EB:** il sistema tpm, ormai implementato su windows 11, blocca questi tentativi di infiltrazione?
   La risposta è stata data on-line da Gianni Amato
2. **MP:** esiste una normativa che impone alle PA di avere al loro interno un responsabile/referente della cybersecurity, ad esempio come il Resp. Sicurezza sul Lavoro?
   La risposta alla domanda sarà approfondita nel 4° Webinar
3. **PS:** nel caso di un attacco ransomware quale responsabilità può essere attribuita al malcapitato ente che viene attaccato? Vista anche la consueta caccia alle streghe che trasforma spesso la vittima in artefice?
   La risposta è stata data on-line da Gianni Amato
4. **PS:** come possiamo controllare se si è presenti negli elenchi mostrati nella slide, ci sono dei siti specifici?
   La risposta è stata data on-line da Gianni Amato
5. **MP**: tutta questa frenesia di muovere sul cloud non rischia di AUMENTARE i rischi per la sicurezza e protezione dei dati?
   La risposta è stata data on-line da Gianni Amato
6. **MP**: esiste un censimento degli Enti che non hanno alcun responsabile della cybersecurity? il recente articolo di AGID non è molto rassicurante.
   La risposta alla domanda sarà approfondita nel 4° Webinar
7. **NN**: si potrebbe attivare un applicativo per segnalare le e-mail di phishing o qualsiasi altro evento di pericolo per la sicurezza informatica? sto parlando di una assistenza aggiuntiva rispetto a quella classica tecnica informatica
   La risposta è stata data on-line da Gianni Amato
8. **LDR**: quali strumenti utilizzare per il test di vulnerabilità di applicazioni web per la PA prima della pubblicazione su web? esistono strumenti freeware o online per la scansione?
   La risposta può essere trova nella slide 30 del modulo Vulnerabilità Software.
9. **LDR**: AGID fornisce materiale per la produzione di software sicuro e non vulnerabile, ma mette a disposizione strumenti per i controlli?
   La risposta alla domanda sarà approfondita nel 4° Webinar – Modulo LG Sviluppo Software Sicuro
10. **AS**: e il dipendente che per distrazione o per incuria favorisce un attacco che responsabilità ha?
    La risposta è stata data on-line da Gianni Amato
11. **DZ**: per standardizzare una strategia in termini di sicurezza minima quali sono le misure da adottare?
    Sono da adottare le misure minime di sicurezza AGID Circolare 2-2017 e anche il principio di accountability del GDPR. Il tema sarà trattato nel 4° Webinar
12. **LDR**: la digitalizzazione dei servizi della PA e l'Open Government, l'Open Data hanno una notevole utilità per gli utenti ma non aumentano in modo considerevole il rischio di attacchi ?
    La risposta è stata data on-line da Gianni Amato
13. **GV:** Cosa rischia una PA ove non è presente né un responsabile sicurezza informatica e/o amministratore di Sistema Informatico?
    La risposta alla domanda sarà approfondita nel 4° Webinar
14. **CG**: Le misure minime di sicurezza fanno riferimento alle relazioni dell'università la Sapienza del 2015. Verranno rilasciate misure minime aggiornate al mondo di oggi?
    La risposta alla domanda sarà approfondita nel 4° Webinar
15. AC: Non tutte le PA hanno la struttura e i soldi per adottare tutte le misure necessarie, né per istituire le necessarie figure. Spesso è tutta teoria, anche per questo si è esposti.
    La risposta alla domanda sarà approfondita nel 4° Webinar – Modulo Strumenti Prevenzione
16. MDA: non sarebbe opportuno "costringere" in qualche modo le PA ad una formazione continua, anche per il personale non specificatamente tecnico?

La risposta alla domanda sarà approfondita nel 4° Webinar

17. AP: come faccio a sapere se un software che ho sviluppato per la pubblica amministrazione è sicuro?
    La risposta alla domanda sarà approfondita nel 4° Webinar – Modulo LG Sicurezza Procurement ICT
18. GS: all'interno dell'ente è previsto la figura dell'amministratore di sistema?
    L'amministratore di sistema, pur non essendo esplicitamente richiamato nel GDPR, ha una considerevole responsabilità sui dati aziendali e riveste un ruolo particolare sul piano operativo all'interno dell'azienda.
19. DZ: Un'architettura 0 trust diffusa potrebbe perlomeno mitigare certi problemi
    Sicuramente un'architettura 0 trust aiuta a mitigare certe tipologie di attacchi. Cmq la risposta sarà approfondita nei prossimi webinar.

BASTI

20. RC: Strumenti di vulnerability scan & management che consigliate? oltre a Nessus naturalmente. Il problema sono sempre i costi per i piccoli comuni
    La risposta può essere trova nella slide 30 del modulo Vulnerabilità Software.
21. **BM:** dovendo affidare un servizio da pubblicare su web con anche dati personali, cosa dobbiamo/possiamo chiedere e pretendere sia dichiarato come garantito nel prodotto ai fini della sicurezza? se non siamo tecnici intendo, come capiamo che il prodotto adotta tutte le policy di sicurezza? Grazie
    La risposta alla domanda sarà approfondita nel 4° Webinar – Modulo LG Sicurezza Procurement ICT
22. **AC:** vengono molto utilizzati dei gestori di password, c'è qualcosa di specifico testato e consigliato da AGID?
    AGID non effettua test su software sviluppati da terze parti. La migliore garanzia di sicurezza è quella di utilizzare password manager standalone.