ASSOCIAZIONE ITALIANA INFORMATION SYSTEMS AUDITORS

nota anche come

ISACA Milan Chapter

MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

ORDINEdegliINGEGNERI della PROVINCIAdiSIENA

PRESENTANO

CYBERARK

Clusit
Associazione Italiana per la Sicurezza Informatica

Cyber Guru

con il patrocinio di

Project Management Institute. Central Italy

CONFASSOCIAZIONI Digital

AIP ITCS

Security Awareness: Conosci il tuo nemico...

26 novembre 2020 14.00-18.00

Sessione di Studio in Streaming

PRESENTAZIONI

Garibaldi Conte, Clusit

Programmi di security awareness: una necessità non più rimandabile

Tutti gli analisti ed esperti di sicurezza concordano che la maggior parte degli incidenti di sicurezza è legata ad errori umani confermando come il fattore umano sia, anche per la sicurezza informatica, l'anello debole del sistema.
Solo in Italia si è stimato che più della metà degli attacchi sono dovuti a cause endogene (utilizzo di password deboli e non alfanumeriche, accesso di device aziendali a connessioni pubbliche, navigazione in siti non sicuri e il trasporto di dati sensibili con chiavi USB non cifrate,…) e a queste si sommano gli attacchi di phishing e spear phishing che provocano impatti significativi sull'azienda sia in termini di frodi e dati rubati che come incremento dei costi operativi per il ripristino dagli incidenti occorsi.
La principale ragione di ciò è legata alla non elevata consapevolezza degli utenti che non è opportunamente formata (o sarebbe meglio dire "consapevolizzata") sui rischi del cyber space. Risulta quindi evidente che la programmazione ed esecuzione programmi di security awareness è diventata una necessità per tutte le aziende non più rimandabile.
Dopo una breve panoramica su quale sia lo stato dell'arte dei programmi di security awareness, l'intervento illustrerà quali siano gli aspetti chiave da curare quando si vuole progettare e realizzare dei programmi di security awareness efficaci.

Massimo Carlotti, CyberArk

Quello che (forse) non sapevate del senso del Privilege Management

Negli ultimi anni si sta affermando la consapevolezza che i confini delle aziende sono sempre più sfumati e le identità stanno diventando il nuovo modo di definirli.
Meno noto che il concetto di identità è indissolubilmente legato ai privilegi di cui dispone. I privilegi sono ovunque, associati ad identità usate da persone fisiche, da applicazioni, robot, tool di orchestrazione, cloud, etc. In questo intervento verranno introdotti elementi di contesto che argomentano la centralità e l'importanza di una corretta gestione dei privilegi.
Verranno chiariti gli aspetti principali che caratterizzano:

- *Perche' occuparsene e quali risultati attendere*
- *Come intervenire*
- *Quali tipi di tecnologie mettere in atto.*

In alcuni brevi approfondimenti verranno illustrati alcuni scenari esemplificativi in ambito:

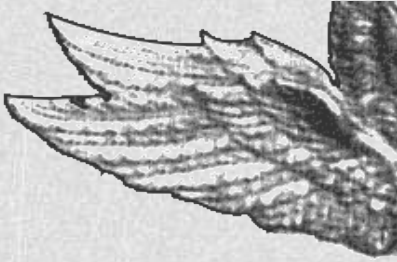
- *Analytics (per capirne i benefici in un approccio integrato)*
- *Endpoint (per contestualizzarlo rispetto a Malware/Ransomware)*
- *Cloud (per introdurre il tema degli "shadow admin").*

Maurizio Zacchi, Cyber Guru

Il fattore umano sotto attacco

La Pandemia da Covid-19 ha avuto importanti riflessi anche sugli attacchi Cyber il cui volume è notevolmente aumentato in questi mesi.
In modo particolare sono aumentati tutti gli attacchi che fanno leva sul fattore umano con dati che si fanno sempre più allarmanti. Su questo dato ha influito certamente il ricorso massivo alla smart working con gli inevitabili effetti di distanziamento sociale e con una maggiore sensibilità degli utenti verso alcune particolari categorie di informazioni.
In ogni caso, questa sorta di contagio virtuale non sembra placarsi e aumentano i casi di organizzazioni colpite da attacchi Malware e Ransomware.
In questo incontro cerchiamo di capire quali sono le principali vulnerabilità del fattore umano e come sono evolute le strategie degli attaccanti, con un focus sulle tecniche di social engineering. Cercheremo anche di capire le contromisure e quindi la necessaria evoluzione delle metodologie che guidano la formazione in ambito Cyber Security Awareness.

AGENDA



14:00 – 14:10

Avvio streaming

14:10 – 14:20

Saluti del Presidente di AIEA

14:20 – 15:10

Garibaldi Conte, Clusit

Programmi di security awareness: una necessità non più rimandabile

15:10 – 16:00

Massimo Carlotti, CyberArk

Quello che (forse) non sapevate del senso del Privilege Management

16:00 – 16:30

Coffee break

16:30 – 17:20

Maurizio Zacchi, Cyber Guru

Il fattore umano sotto attacco

17:20 – 18:00

Confronto e dibattito

18:00

Conclusione e ringraziamenti

RELATORI

Garibaldi Conte, Clusit

Dopo aver conseguito la Laurea in Scienze della Informazione, ha lavorato per circa 20 anni in CSELT, Telecom Italia, Tibercom ed Elitel dove ha sviluppato una significativa esperienza professionale in ambiti ICT e Sicurezza ICT gestendo progetti complessi e partecipando allo start up di numerose iniziative. Da circa 15 anni opera come consulente nell'ambito della Sicurezza ICT collaborando con le principali società di consulenza operanti in tale mercato. Ha gestito importanti progetti di sicurezza ICT su varie tematiche quali Compliance, Risk Management, Incident Handling per conto di grandi aziende nazionali e internazionali operanti in vari settori (Finanza, Telecomunicazioni, Pubblica Amministrazione, …). Dal 2018 è co-fondatore e Managing Director di Atsec Information Security srl, società appartenente ad un network internazionale e operante nella certificazione di sicurezza dei prodotti ICT. È membro del Comitato Scientifico del Clusit.

Massimo Carlotti, CyberArk

Sales Engineer da oltre 15 anni, ha trascorso i suoi primi anni di esperienza professionale in Siemens Business Services, dove ha ricoperto ruoli di Consultant, Business Developer e Presales.
Entra nel 2007 a far parte del team dei Sales Engineer di RSA e si occupa prevalentemente di affiancare i partner del Canale in Italia su tematiche di Strong Authentication, SIEM e DLP.
Tra il 2011 ed il 2016 diventa un senior Sales Engineer in ARROW ECS (ex Computerlinks) per contribuire al rafforzamento delle attivita' di prevendita e contribuire a mantenere la leadership di Distributore a Valore Aggiunto. In questi anni ha modo di portare avanti le sue precedenti competenze ed approfondire altre tematiche e proposizioni quali WAN Optimization (Riverbed), SIEM (ArcSight), IPS (TippingPoint) ed altro ancora.
Convinto di non saperne mai abbastanza ed innamorato della Prevendita, da inizio 2017 torna nel mondo dei Vendor ed entra come Sales Engineer a far parte del team di prevendita di CyberArk per la regione South EMEA.
Ad inizio 2020 diventa PreSales Team Leader per CyberArk in Italia.

RELATORI

Maurizio Zacchi, Cyber Guru

Negli oltre 30 anni di esperienza lavorativa maturati interamente nel settore ICT, ha ricoperto molti ruoli, acquisendo una visione completa delle reali esigenze delle grandi organizzazioni italiane, sia del settore pubblico che privato. In questo senso ha seguito l'intera evoluzione del settore della Cyber Security. Dal 2016 ha avviato una collaborazione stabile con il Gruppo Daman, società italiana specializzata in ambito Cyber, assumendo il ruolo di Marketing Manager. Dal 2017 ha partecipato direttamente allo sviluppo del progetto Cyber Guru che si è concretizzato nel rilascio di piattaforme avanzate di Cyber Security Awareness. In questo ambito, oltre a ricoprire l'incarico di Marketing Manager, ha assunto la responsabilità del team multidisciplinare che si occupa della produzione dei contenuti formativi, un incarico che gli ha permesso di consolidare le proprie conoscenze sia nel settore della Cyber Security sia nel settore della formazione e della comunicazione.

ISCRIZIONE

Soci AIEA

*L'iscrizione all'evento, gratuita, deve essere completata sul Portale delle Sessioni di Studio AIEA, all'indirizzo **https://portale.aiea.jed.st/** entro e non oltre il 25 novembre 2020. La partecipazione all'evento dà diritto ad acquisire 4 CPE per mantenere le certificazioni CISA, CISM, CGEIT e CRISC.*

Ordine degli Ingegneri

*L'iscrizione all'evento deve essere completata sul portale della Formazione Continua dell'Ordine degli Ingegneri della Provincia di Siena **http://siena.ing4.it/**. La partecipazione all'evento dà diritto ad acquisire **3 CFP**.*

*La partecipazione all'evento richiede un contributo di **5 Euro**.*

Non Soci

*La partecipazione all'evento richiede un contributo di **10 Euro**. Per iscriversi contattare la Segreteria AIEA all'indirizzo email aiea@aiea.it entro e non oltre il 25 Novembre 2020.*

*L'evento è **gratuito per gli studenti** e **per i soci delle associazioni patrocinanti.***

ISACA®

Milan Chapter

ORDINE degli INGEGNERI della PROVINCIA di SIENA

L'Ordine è un Ente pubblico Non Economico, ausiliario dello Stato, istituito con Legge Ordinaria.

All'Ordine sono attribuite specifiche competenze; è sottoposto al controllo ed alla vigilanza da parte del Ministero di Grazia e Giustizia, presso il quale è stabilita la sede del Consiglio Nazionale CNI

L'Ordine tiene aggiornato l'elenco degli iscritti nell'Albo Professionale.

La professione di Ingegnere, nei sui vari indirizzi, rientra tra le cosiddette professioni protette; ciò significa che per essere legittimati ad esercitare è necessaria l'iscrizione al relativo albo.
L'Ordine professionale da un lato si fa garante dell'accesso all'esercizio della professione di Ingegnere solo da parte di soggetti in possesso dei requisiti richiesti dalla legge, dall'altro lato esercita controllo sui propri iscritti, richiedendo loro che mantengano un comportamento rispondente alla deontologia professionale.

L'Ordine è totalmente sostenuto dai contributi degli iscritti, conferiti provincia per provincia

http://ording.si.it/

Ordine degli Ingegneri della Provincia di Siena
info@ording.si.it

Associazione Italiana Information Systems Auditors

L'Associazione Italiana Information Systems Auditors è stata costituita a Milano nel 1979 con lo scopo di promuovere l'approfondimento dei problemi connessi con il controllo del processo di elaborazione automatica dei dati e di favorire lo sviluppo di metodologie e tecniche uniformi per la loro soluzione.

In particolare, gli obiettivi dell'Associazione sono:

- promuovere un processo di sensibilizzazione di tutti i livelli organizzativi aziendali alla necessità di stabilire adeguati criteri di controllo, di affidabilità dell'organizzazione, Information Systems e di sicurezza dei sistemi;
- ampliare la conoscenza ed esperienza dei suoi oltre 800 membri nel campo dell'IT Governance, IT Security, Information Systems Auditing e Risk Control, favorendo lo scambio di metodologie per lo studio e la soluzione dei problemi inerenti;
- promuovere a livello nazionale la partecipazione alla certificazioni CISA, CISM, CGEIT, CRISC, CobiT e CSX

AIEA è associata da 40 anni ad ISACA, primo Capitolo in Europa, diventando nota internazionalmente come

ISACA® Milan Chapter

ISACA® per i suoi oltre 135,000 soci in 188 paesi e per la comunità dei professionisti IT è fonte affidabile di possibilità di networking, certificazioni professionali, conoscenza e standard negli ambiti IT Governance, Cybersecurity, IT Risk e Assurance

www.aiea.it

20123 Milano - Via privata del Gonfalone, 3 - E-mail: aiea@aiea.it
Sito web: www.aiea.it – www.isaca.mi.it - P.IVA n. 10899720154 - C.F. n. 97109000154