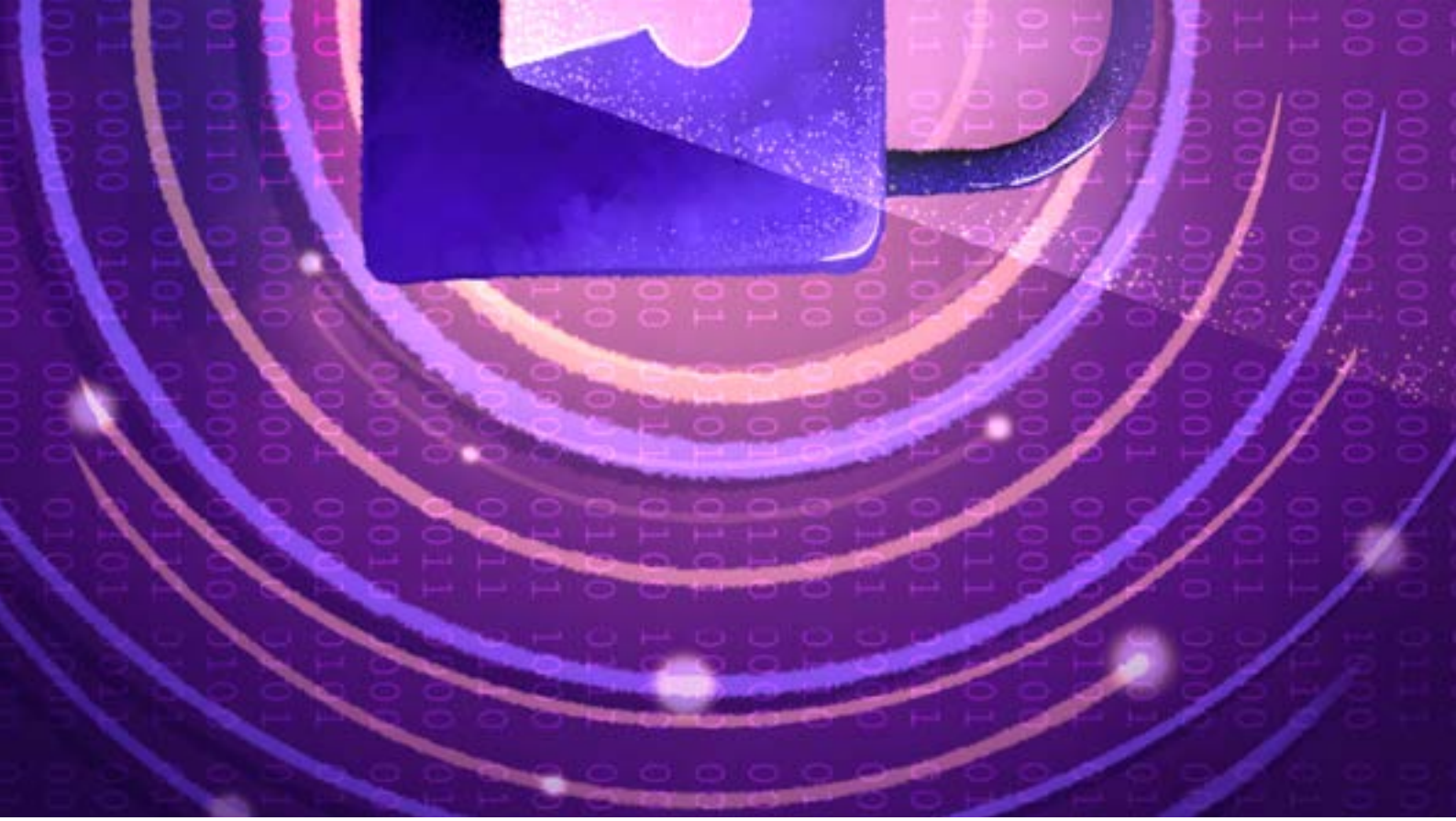


CYBER SECURITY

WHITE PAPER

CODING THE FUTURE

Certificazioni

Autori


Marco Mehanna
SECURITY ADVISOR


Roberto Bindi
SECURITY ADVISOR


Gaia Conti
LEAD EDITOR


Ariele Pirona
VISUAL GRAPHICS

Indice

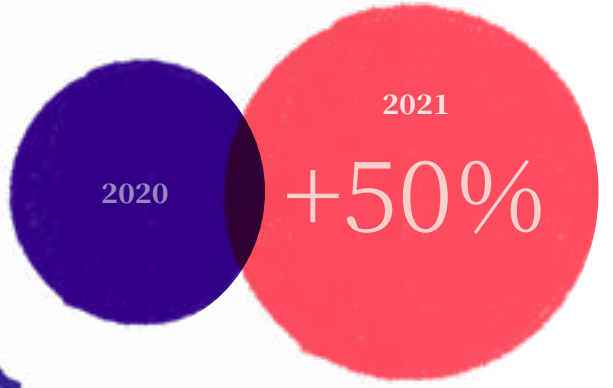
NUMERI

Come diceva un vecchio detto, l'unico modo per mantenere un computer completamente sicuro è spegnerlo. E anche questo potrebbe non essere sufficiente oggi, visto che la maggior parte dei dispositivi è connessa a Internet.

La realtà è che una sicurezza perfetta (che implica la certezza assoluta di zero perdite) sarebbe infinitamente costosa e poco pratica. L'obiettivo della gestione del rischio è quello di ottimizzare l'allocazione delle risorse riducendo al minimo sia il costo della sicurezza che le perdite di rischio subite.

La crisi legata alla pandemia COVID-19 ha dimostrato quanto Internet e i computer in generale siano importanti per le organizzazioni e le aziende di qualsiasi dimensione per mantenere la propria operatività. Per sopravvivere alla pandemia e continuare l'attività, molte hanno dovuto adottare misure di continuità aziendale come l'adozione di servizi cloud, l'aggiornamento dei servizi Internet, il miglioramento dei siti web e la possibilità per il personale di lavorare da remoto. Per questi motivi, la pandemia ha posto ulteriori sfide alla sicurezza informatica.

ATTACCHI HACKER



Nel 2021 le organizzazioni hanno subito il 50% in più di attacchi settimanali rispetto al 2020.

IN ITALIA

5000
Attacchi al mese

167
Al giorno

7
All'ora

Ogni volta che si sente la parola Hacking, la prima cosa che si pensa è che si tratti di pratiche informatiche dannose.
Ma non è così.
Non esistono hacker buoni o cattivi. Esistono professionisti della security e criminali informatici.

LA NOSTRA CASE HISTORY

SECURITY RESEARCH

Avere un approccio etico ci ha consentito di scoprire numerose vulnerabilità in molti sistemi come quello individuato a fine 2017: un difetto su un componente del sistema di comunicazione anonimo internazionale, The Onion Router, noto come Tor Browser. Nello specifico, Interlogica ha identificato un bug all'interno del software che consentiva a terze parti di scoprire le identità degli utenti. Questo bug è stato poi identificato come TorMoil, comunicato all'azienda e corretto.

Un messaggio "distorto" mandava in shut-down Gmail, il più famoso web mail del mondo.

Per gli utenti Mac con Microsoft RDC installato abbiamo rilevato un bug sull'esecuzione del codice in modalità remota

Questo bug da noi rilevato interessava i dispositivi Mac OS X. Un Javascript locale abilitava il bypass della quarantena.

Abbiamo rilevato una anomalia su SquirrelMail sul quale è risultata possibile l'esecuzione di codice da remoto.

ADOTTA IL GIUSTO APPROCCIO

6 CONSIGLI PER PROTEGGERE AL MEGLIO L'AZIENDA

1

MANTIENITI AGGIORNATO SULLE LEGGI

Le leggi su privacy e riservatezza sono in continua evoluzione. Ad esempio, storage e gestione dati devono essere conformi a regolamenti come GDPR. L'aggiornamento continuo aumenta la consapevolezza informatica, e evita anche costose sanzioni per non conformità in caso di violazione.

2

APPLICA UNA PASSWORD POLICY

L'autenticazione, dove possibile, deve essere centralizzata. Ciò significa gestire gli accessi attraverso strumenti di Identity Access Management su cui deve essere applicata una corretta policy sulla robustezza delle password.

3

APPLICA STANDARD DI SVILUPPO SICURO

Accertati che i software prodotti dalla propria azienda e i software in utilizzo vengano sviluppati seguendo linee guida di sviluppo sicuro (es. OWASP Secure Coding Practices) e buone pratiche dell'SDLC.

4

SEGREGAZIONE DEGLI AMBIENTI

Suddividi la rete interna in più sottoreti, ognuna con policy di sicurezza e protocolli specifici; questo è il primo passo verso la prevenzione dal movimento laterale. È una delle pratiche più utilizzate per limitare la superficie di attacco e contrastare attacchi informatici.

5

AGGIORNA SOFTWARE E FIRMWARE

Mantieni sistemi e applicativi aggiornati all'ultima versione rilasciata dal fornitore. Questa pratica deve essere eseguita con regolarità, avvalendosi di un processo interno di Patch Management e/o di sistemi per l'aggiornamento automatico.

6

MONITORAGGIO

Costruire una strategia di monitoraggio per sistemi ICT e network e sviluppare politiche di gestione degli alert. Analizzare i log con lo scopo di scovare attività inusuali che denotino un attacco.

COSA POSSIAMO FARE PER TE

CYBER SECURITY

I NOSTRI SERVIZI

SICUREZZA PREDITTIVA

CYBER THREAT INTELLIGENCE

Identifichiamo le minacce provenienti da attività illecite di esfiltrazione dirette e indirette. Un valido supporto nel tenere monitorata costantemente e nel tempo la sicurezza dell'organizzazione mediante prevenzione.

SECURITY AWARENESS

Sensibilizziamo e rendiamo consapevoli le persone nel riconoscere varie tipologie di minacce e le possibili conseguenze, prima che vadano a buon fine.

SICUREZZA PROATTIVA

PENETRATION TEST

Rileviamo e classifichiamo, attraverso attività di analisi manuale, le criticità potenzialmente sfruttabili da agenti malevoli. Il test del sistema avviene tramite un attacco simulato e approfondito.

CODE REVIEW

Analizziamo il codice sorgente di un'applicazione per identificare potenziali vulnerabilità dal punto di vista infrastrutturale e logico. Per farlo usiamo sia tool di Code Review che l'intervento di uno dei nostri esperti.

COMPLIANCE

SUPPORTO SISTEMISTICO

Diamo assistenza nella valutazione e miglioramento della compliance degli standard GDPR, e nel hardening dei sistemi (sia software che hardware), per ridurre quanto più possibile i rischi per la sicurezza.

VULNERABILITY ASSESSMENT

Identifichiamo e classifichiamo per gravità le componenti aziendali affette da vulnerabilità note.

RED TEAMING

Cerchiamo vulnerabilità informatiche (e non) di un'azienda attraverso un team dedicato che, oltre a sfruttare le debolezze software, utilizza anche tecniche di Social Engineering e altri tipi di attacchi per violare il perimetro.

KNOWBE4

SOLUTION PARTNER

Grazie alla partnership con KnowBe4 siamo in grado di offrire dei servizi di semplice utilizzo, gratuiti ed efficaci!

KnowBe4 è la prima e più grande piattaforma al mondo per la formazione di Security Awareness e per la simulazione del Phishing.

Un team di professionisti della tecnologia che guardano ai problemi di sicurezza informatica da un punto di vista differente, valorizzando la sicurezza attraverso un solido firewall umano.

Dal 2019 è inserita nel Magic Quadrant di Gartner che nel 2021 la conferma come Peer Insights™ Customers' Choice per la qualità della formazione IT sulla Security Awareness.

STRUMENTI GRATUITI PER LA SICUREZZA IT

Metti alla prova le persone che lavorano in azienda con gli strumenti gratuiti per la sicurezza informatica, che aiutano a identificare i problemi di Social Engineering, Spear Phishing e attacchi Ransomware.

Phishing Security Test
Il 91% delle violazioni di dati inizia con un attacco di spear phishing. Con questo test, puoi scoprire quanti dipendenti sono soggetti a phishing.

Breached Password test
Il 25% dei dipendenti utilizza la stessa password per tutti gli accessi. Verifica se i tuoi utenti stanno utilizzando password già violate e agisci rapidamente.

Ransomware Simulator
La protezione degli endpoint blocca effettivamente le infezioni da ramsomware e cryptomining? "RanSim" verifica rapidamente l'efficacia della protezione esistente.

Email Exposure Check Pro

Le credenziali dei tuoi dipendenti sono compromesse? Questo tool identifica gli utenti a rischio nella tua organizzazione, analizzando migliaia di database sulle violazioni.

Mail Security Assessment
L'e-mail è ancora il primo vettore di attacco utilizzato dai malintenzionati. Il MSA verifica l'efficacia del tuo mail server nel gestire il filtraggio della posta.

Domain Doppelgänger

Identifica e monitora i domini potenzialmente dannosi che possono essere sfruttati per falsificare il tuo dominio.

Automated Security Awareness Program
Crea un programma di sensibilizzazione alla sicurezza per la tua organizzazione con attività, suggerimenti utili e contenuti formativi.

Modstore Preview Portal

La più grande libreria al mondo di contenuti formativi sulla consapevolezza della sicurezza informatica con più di mille moduli interattivi, video, giochi, poster e newsletter.


CASE
STUDY

CASE STUDY

TRUFFA DELL'AMMINISTRATORE DELEGATO

La truffa del CEO si verifica quando un Dirigente e/o un dipendente autorizzato ad effettuare pagamenti, viene indotto a pagare una fattura falsa oppure ad effettuare un trasferimento non autorizzato dall'account aziendale.

QUALI SONO I SEGNALI?

- Email/telefonata indesiderata
- Contatto diretto da un alto funzionario con il quale non si è normalmente in contatto
- Richiesta di riservatezza assoluta
- Pressione e senso di urgenza
- Richiesta insolita in contrasto con le procedure interne
- Minacce o adulazioni inusuali/promesse di ricompensa

COSA PUOI FARE?

COME AZIENDA

- Sii consapevole dei rischi e assicurati che anche i tuoi dipendenti siano informati.
- Invita il tuo staff a trattare le richieste di pagamento con cautela.
- Implementa protocolli interni relativi ai pagamenti.
- Implementa una procedura per verificare la legittimità delle richieste di pagamento ricevute via email.
- Stabilisci un processo di segnalazione per la gestione delle frodi.
- Rivedi le informazioni pubblicate sul sito web della tua azienda, limita le informazioni e sii prudente sui social media.
- Incrementa e aggiorna la sicurezza tecnologica.

COME IMPIEGATO

- Applica rigorosamente le procedure di sicurezza in vigore per i pagamenti e le forniture. Non saltare alcun passaggio e non cedere alla pressione.
- Controlla sempre attentamente gli indirizzi email quando si tratta di dati personali o di fatturazione.
- In caso di dubbio su un ordine di trasferimento, consulta un collega competente.
- Non aprire mai link sospetti o allegati ricevuti tramite email. Evita di controllare la tua email privata sui computer aziendali.
- Limita le informazioni e sii prudente sui social media.
- Evita di condividere informazioni sulla strutturainterna, sulla sicurezza o sulle procedure dell'azienda.

CYBER SECURITY

CASE STUDY

DATA BREACH

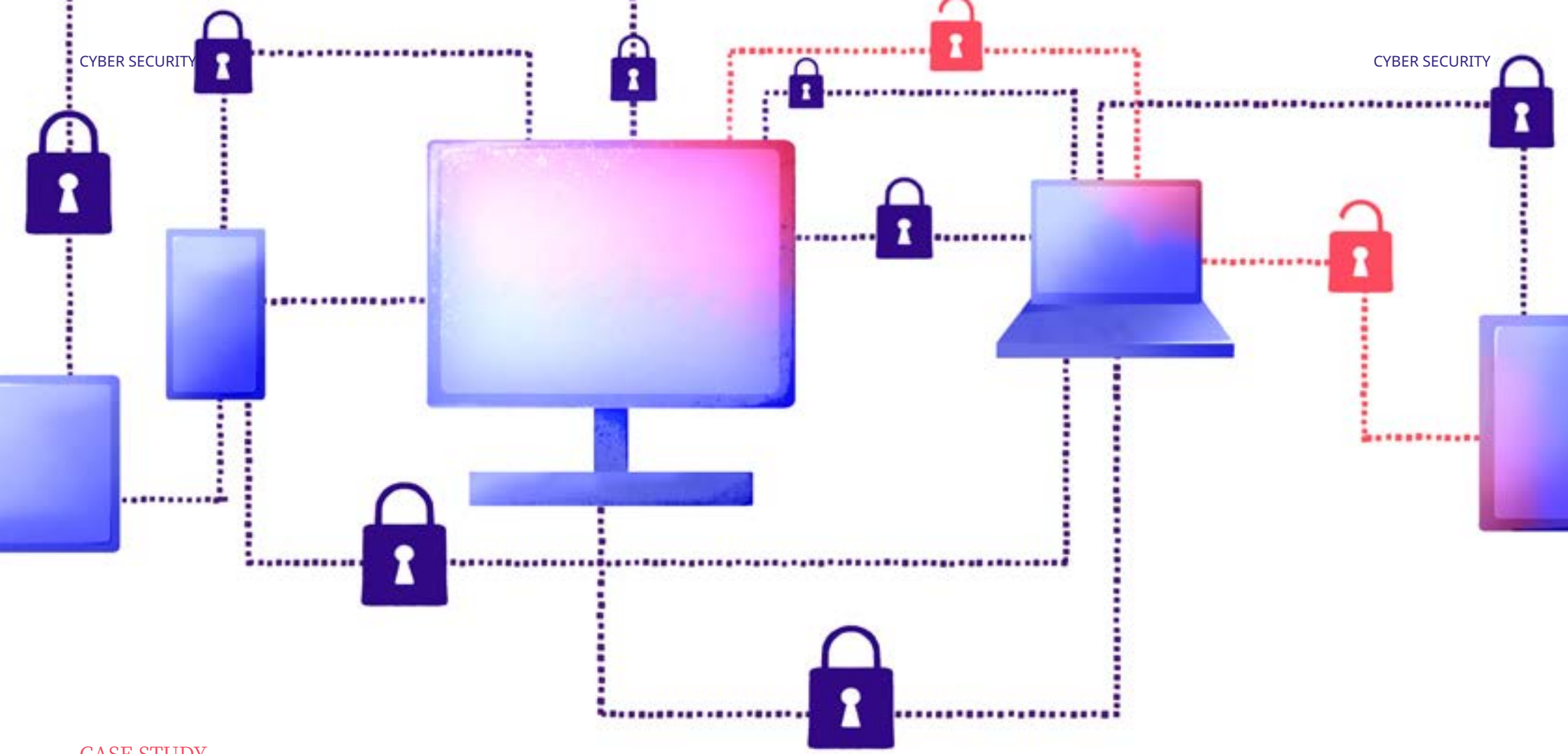
L’azienda subisce un'importante esfiltrazione di dati, resi successivamente pubblici su internet. A seguito di indagini, emerge che gli attaccanti sono rimasti all’interno dell’infrastruttura informatica per mesi e, a causa di un’insufficiente sicurezza perimetrale e l’assenza di sistemi di monitoraggio, è stato scoperto al momento della pubblicazione dei dati.

COSA PUOI FARE?

COME AZIENDA

- Dota l'azienda di sistemi di protezione perimetrale e di monitoraggio
- Applica politiche di segregazione della rete, così da evitare che l’attaccante possa muoversi liberamente sulla rete interna.
- Esegui attività di Red Teaming. Rivolgiti quindi a un gruppo di esperti che simuleranno, attraverso scenari d’attacco reali, un’intrusione informatica all’interno del perimetro aziendale. Questo, con lo scopo di identificare possibili debolezze ed eseguire un’accurata valutazione del rischio.

CYBER SECURITY



CASE STUDY

VULNERABILITÀ NOTE

L'infrastruttura aziendale è stata parzialmente compromessa, sia a livello di integrità che di disponibilità dei servizi offerti. Gli applicativi presenti in azienda utilizzano prevalentemente il framework Struts e la versione installata è affetta da una vulnerabilità nota, dalla criticità elevata e facilmente sfruttabile.

COSA PUOI FARE?

COME AZIENDA

- Implementa un Web Application Firewall a protezione dell'infrastruttura.
- Esegui attività di Vulnerability Assessment allo scopo di identificare vulnerabilità note presenti sulle componenti utilizzate.
- Implementa un processo di Patch Management, così da eseguire in maniera strutturata aggiornamenti su tutte le componenti utilizzate.
- Esegui periodicamente attività di Penetration Test sia sugli applicativi che sui server nei quali risiedono.
- Effettua un'analisi del codice sorgente prima di ogni rilascio in produzione.

GLOSSARIO

ANTIVIRUS

L'antivirus è un'applicazione software che aiuta a proteggere il computer dai virus. È una raccomandazione standard per ogni computer, indipendentemente dal fatto che si tratti di un computer aziendale o personale. Di solito sono dotati di protezione:

- Multi Device, ovvero possono essere utilizzati per proteggere il computer, il cellulare e il tavolo.
- Multi Threat Protection, ovvero protezione da diversi tipi di minacce informatiche.
- Parental Control, consente di controllare ciò che i vostri figli possono fare sul vostro computer.
- Firewall, che aggiunge un livello di difesa tra computer e Internet.
- Uno strumento di rimozione dei virus per aiutarvi se il vostro computer viene infettato.

CRITTOGRAFIA

La crittografia è una forma di protezione dei dati. Il processo di crittografia prevede l'uso di codici e chiavi complesse per criptare o bloccare i dati, rendendoli quasi inutili a meno che non si disponga della chiave per decifrarli o sbloccarli. Si tratta di un modo protetto di trasferire informazioni sensibili e di tenere al sicuro il computer fisico. Se il computer viene rubato, è quasi impossibile recuperare i dati dal disco rigido se questo è stato criptato (a condizione che siano state adottate le giuste misure di protezione con password). La crittografia può essere utilizzata anche per scopi dannosi. I criminali informatici che eseguono attacchi Ransomware utilizzano metodi di crittografia per bloccare i file.

—

CYBER THREAT INTELLIGENCE

La Cyber Threat Intelligence rappresenta lo strumento che consente di adottare strumenti di difesa specifici per i possibili attacchi e individuare eventuali nuovi punti deboli all'interno della rete aziendale. Per garantire la sicurezza delle aziende è necessaria un'intensa attività di Cyber Threat Intelligence che consenta di prevenire gli attacchi da parte dei criminali informatici. di sicurezza degli asset che compongono.

—

DATA BREACH

Un Data Breach - violazione dei dati - ha luogo quando i dati, personali o aziendali. sono stati compromessi, un hacker ne ha avuto accesso. Cosa può fare con i dati? Li può vendere sul dark web, può bloccarne l'accesso tramite una sorta di cryptolocker o semplicemente è riuscito ad avere accesso ai tuoi sistemi e sta inserendo spyware. Qualunque sia la ragione, qualsiasi tipo di accesso malevolo ai sistemi viene definito violazione dei dati.

—

FIREWALL

Un firewall funge da barriera tra il computer e Internet. Aiuta a mantenere al sicuro il computer e i dati in esso memorizzati. Esistono diversi tipi di firewall, come i dispositivi fisici che si affiancano al router o al modem e i firewall virtuali o ospitati nel cloud, che rappresentano un livello di protezione software. Windows e Mac sono dotati di funzionalità di firewall integrate, il che è un ottimo inizio, ma come azienda è importante investire anche in un firewall di livello corporate.

—

HUMAN FIREWALL

L'elemento umanodella cybersecurity. La tecnologia può fare molto per proteggere te e la tua azienda, ma è fondamentale educare le persone a identificare una potenziale truffa. Una via per colmare questa lacuna è coniugare processo e tecnologia, fornendo regolarmente contenuti educativi. Assicurati che le persone sappiano come identificare un tentativo di attacco informatico, prima di cliccare su un link o prima di fornire una password al telefono, e che sappiano distinguere tra un sito web affidabile da uno che no lo è.

PENETRATION TEST

Il Penetration Test, spesso abbreviato in Pentest, è una prova di valutazione del livello di sicurezza degli asset che compongono il perimetro aziendale, tra cui server, applicazioni web e mobile. Questo tipo di analisi aiuta a trovare le lacune negli strumenti di sicurezza che un'organizzazione sta usando, trova più vettori di attacco e problemi di configurazione.

—

PHISHING

Il phishing è un tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale. Solitamente inizia con una e-mail o un'altra comunicazione fraudolenta inviata allo scopo di attirare una vittima.

—

RANSOMWARE

Il ransomware (talvolta indicato come cryptolocker) consiste in un semplice virus che, una volta entrato nel computer o nella rete aziendale, cripta i file rendendoli inutilizzabili senza una chiave di decrittazione. Non solo i grandi marchi sono un bersaglio, le piccole imprese sono tra le più vulnerabili agli attacchi ransomware. Spesso i proprietari di PMI pensano di essere troppo piccoli per essere un obiettivo e questo è il motivo per cui molti hacker li prendono di mira.

—

SECURITY AWARENESS

La Security Awareness è la conoscenza e l'atteggiamento che le persone di un'organizzazione hanno nei confronti della protezione delle risorse fisiche e, soprattutto, informatiche dell'organizzazione stessa. È fondamentale in ciascuna azienda rendere consapevoli le persone nel riconoscere varie tipologie di minacce e le possibili conseguenze prima che vadano a buon fine.

SOCIAL ENGINEERING

Questo tipo di reato informatico si basa esclusivamente sulla manipolazione delle vittime da parte dei criminali informatici, che sfruttano la naturale inclinazione alla fiducia delle persone. Le informazioni prese di mira variano, ma in genere si tratta di password, dati bancari o altre informazioni personali.

—

VULNERABILITÀ

Il termine vulnerabilità viene usato spesso nel mondo della cybersecurity e si riferisce a così tanti aspetti diversi della sicurezza informatica che a volte può sembrare privo di significato, ma è un termine importante. Si riferisce a tutte le aree della cybersecurity in cui potreste essere vulnerabili a un attacco informatico. Potrebbe trattarsi di una patch di sicurezza mancante, di un software non aggiornato o di un'area della vostra azienda che necessita di maggiore formazione in materia di cybersecurity. In sostanza, tutto ciò che viene segnalato come "vulnerabile" nella vostra suite tecnologica deve essere affrontato come priorità.

WE ARE INTERLOGICA

Siamo un'azienda specializzata nella consulenza tecnologica che integra strategia e software.
Costruiamo con te un percorso unico, ti supportiamo nella progettazione, implementazione e gestione di una varietà di ambienti IT che ti aiutino a navigare in un mercato in continua evoluzione.

Seguici su

in company/Interlogica
@interlogici
@Interlogica

Maggiori informazioni

interlogica.it
info@interlogica.it

Certificazioni

CSQ ISO 9001 CSQ ISO/IEC 27001

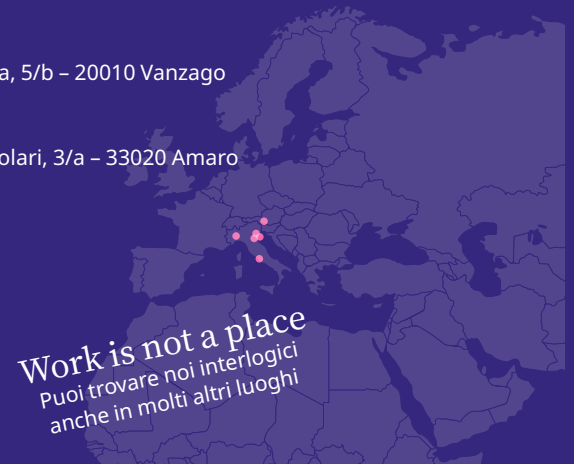
Contatti e sedi

Venezia – Mestre
Via Miranese, 91/4 – 30174, Mestre (VE)
+39 041 5354800

Roma
Via G. Coppola di Musitani 34 · 00139 Roma

Milano
Via Pregnana, 5/b – 20010 Vanzago

Udine
Via Fratelli Solari, 3/a – 33020 Amaro



Work is not a place
Puoi trovare noi interlogici anche in molti altri luoghi

Contatta i nostri esperti

Potenzia la tua strategia e investi in Difesa, Consapevolezza e Conoscenza per sviluppare una cultura della cyber-sicurezza.

Interlogica

CODING THE FUTURE

interlogica.it