Deas, hacker italiani a difesa del patrimonio artistico

Descrizione

default watermark

(Adnkronos) â?? Un museo oggi Ã¨ anche una rete. Dietro le sale, le opere e gli spazi aperti al pubblico esiste unâ??infrastruttura fatta di sistemi di videosorveglianza Ip, controllo degli accessi, archivi digitali, sensori ambientali, dispositivi connessi e piattaforme per la gestione delle collezioni. La trasformazione digitale ha cambiato profondamente il modo in cui il patrimonio culturale viene conservato, studiato e reso accessibile. Ha anche introdotto nuove superfici di rischio, proprio mentre sta cambiando la criminalitÃ che prende di mira musei, collezioni e opere dâ??arte. Ã? su questo terreno che Deas vuole portare una visione maturata negli anni nel mondo della cybersecurity italiana: valorizzare la cultura hacker e mettere le sue migliori competenze al servizio degli asset strategici del Paese. Una cultura hacker lontana dagli stereotipi. Per Stefania Ranzato significa prima di tutto talento, creativitÃ , capacitÃ di leggere un sistema fuori dagli schemi, trovare ciÃ² che gli altri non vedono e immaginare soluzioni impreviste. Una componente umana, e per certi versi artistica, che Deas ha scelto di coltivare come parte della propria identitÃ . Oggi quella stessa cultura puÃ² diventare uno strumento per proteggere uno dei patrimoni piÃ¹ preziosi dellâ??Italia.

I nuovi ladri dei musei. Anche il furto dâ??arte sta cambiando.

Un recente rapporto Europol sui furti di beni culturali, ripreso da Artuu, descrive un panorama criminale molto diverso dallâ??immaginario classico del ladro dâ??arte specializzato. Accanto alle organizzazioni strutturate compaiono gruppi temporanei reclutati attraverso social network e servizi di messaggistica, assemblati intorno a una singola operazione. Competenze, uomini e mezzi possono essere reperiti e aggregati per lâ??occasione secondo una logica che Europol riconduce al cosiddetto crime as a service. Gruppi meno stabili, responsabilitÃ piÃ¹ difficili da ricostruire e modalitÃ operative che possono essere estremamente violente. Gli episodi europei degli ultimi anni raccontano bene il fenomeno: teche distrutte con martelli e asce, esplosivi utilizzati per accedere alle collezioni, opere e oggetti preziosi sottratti anche per essere smontati o fusi. In alcuni casi il valore culturale dellâ??oggetto diventa secondario rispetto alla possibilitÃ di trasformarne rapidamente i materiali in denaro. Anche lâ??Italia Ã¨ interessata dal fenomeno. Musei pubblici, fondazioni e collezioni private costituiscono un patrimonio enorme e diffuso, spesso custodito allâ??interno di edifici storici nei quali le esigenze di sicurezza devono convivere con quelle di conservazione, accessibilitÃ e fruizione. A questa evoluzione della minaccia si aggiunge la crescente componente tecnologica delle strutture da

proteggere.

Il museo come infrastruttura connessa

La sicurezza di un museo non si esaurisce piÃ¹ nella protezione delle sale. Una telecamera Ã¨ un dispositivo connesso. Un sistema di controllo degli accessi dialoga con una rete. Gli archivi delle collezioni sono digitali. Sensori e sistemi antintrusione raccolgono e trasmettono informazioni. Il personale utilizza account, credenziali, dispositivi e piattaforme. Una vulnerabilitÃ informatica puÃ² quindi produrre conseguenze che vanno oltre la sottrazione di dati. PuÃ² riguardare la continuitÃ operativa, la disponibilitÃ dei sistemi, la sicurezza delle informazioni e, in determinate circostanze, lâ??interazione tra infrastruttura digitale e dispositivi fisici. Per Deas, proteggere il patrimonio culturale significa cominciare a considerare questa dimensione come parte integrante della sua sicurezza. â??Arte e cultura sono asset strategici del Paese e dobbiamo iniziare a proteggerli anche come tali â?? spiega Stefania Ranzato â?? In Deas stiamo lavorando molto sulla valorizzazione culturale della figura dellâ??hacker, anche nella sua componente piÃ¹ creativa e dirompente. Parliamo di giovani talenti capaci di guardare un sistema da prospettive diverse, individuare una vulnerabilitÃ e trovare soluzioni che difficilmente possono essere standardizzate. Ã? una capacitÃ preziosa per la cybersecurity italiana e puÃ² esserlo anche per la tutela del nostro patrimonio culturaleâ?•.

default watermark

La cultura hacker al servizio del Paese

Deas Ã¨ stata tra le realtÃ italiane che hanno scelto di investire sulla componente offensiva della cybersecurity e sulla valorizzazione dei talenti hacker, riconoscendo nel loro modo di pensare una risorsa che va oltre la singola competenza tecnica. Pensare come un attaccante significa osservare un sistema cercando percorsi inattesi, punti deboli, configurazioni trascurate e combinazioni che una verifica ordinaria potrebbe non intercettare. Penetration test, vulnerability assessment, red teaming e simulazioni controllate permettono di sottoporre le infrastrutture a verifiche realistiche. Cyber threat intelligence e analisi delle informazioni disponibili consentono invece di osservare lâ??evoluzione delle minacce e comprenderne in anticipo tecniche e comportamenti. Applicate al patrimonio culturale, queste capacitÃ possono contribuire alla costruzione di modelli di protezione nei quali sicurezza fisica e digitale siano pensate insieme. Resta centrale il fattore umano. Direttori, personale amministrativo, addetti alla sicurezza e tecnici fanno parte dello stesso sistema. Una credenziale compromessa, un accesso configurato male o una comunicazione fraudolenta possono vanificare investimenti tecnologici importanti. Tecnologia, competenze offensive e formazione devono quindi essere integrate allâ??interno di una cultura condivisa della protezione. â??Stiamo lavorando perchÃ© questa visione possa tradursi anche in iniziative concrete â?? prosegue Ranzato â?? Vogliamo promuovere una cultura della cyber offensive al servizio del patrimonio culturale e lavorare alla sottoscrizione di protocolli dâ??intesa con i musei. Lâ??Italia custodisce un patrimonio unico al mondo e oggi una parte della sua protezione passa inevitabilmente anche dal dominio cyberâ?•.

Una difesa che unisce competenze diverse

Lâ??Italia dispone giÃ di competenze istituzionali di assoluto rilievo nella tutela dei beni culturali. Il Comando Carabinieri per la Tutela del Patrimonio Culturale rappresenta da decenni un punto di riferimento nella prevenzione e nel contrasto dei reati contro lâ??arte e dispone oggi anche di competenze dedicate alla Cyber Investigation. Lâ??evoluzione delle minacce rende sempre piÃ¹

EI SRL - P.IVA IT16017671005

importante la capacitÃ di far dialogare, nel rispetto dei diversi ruoli, esperienza istituzionale, ricerca, cultura e industria della cybersecurity. Per Deas questo dialogo puÃ² essere ulteriormente sviluppato portando nel sistema della tutela culturale competenze maturate nella difesa degli altri asset strategici del Paese.

Due patrimoni italiani

Lâ??Italia custodisce musei, aree archeologiche, biblioteche, archivi, chiese, palazzi storici e collezioni che costituiscono una parte irripetibile della sua identitÃ e della sua rilevanza nel mondo. Allo stesso tempo, negli ultimi anni Ã¨ cresciuta una generazione di professionisti della cybersecurity con competenze offensive di altissimo livello. Giovani capaci di muoversi dentro sistemi complessi, comprenderne le logiche e metterle alla prova. Deas ha scelto di investire su questo capitale umano e sulla sua cultura. â??Quando parliamo di hacker, mi interessa soprattutto la capacitÃ di pensare in maniera diversa â?? conclude Stefania Ranzato â?? Ã? una forma di talento che abbiamo il dovere di riconoscere, coltivare e mettere al servizio del Paese. Oggi vogliamo portare questa capacitÃ anche nel mondo dellâ??arte e della cultura. Difendere il patrimonio italiano significa proteggere qualcosa che appartiene alla nostra storia, alla nostra identitÃ e al nostro futuroâ?•. Mettere i migliori talenti cyber a difesa dellâ??arte significa far incontrare due patrimoni italiani: quello che abbiamo ricevuto dalla nostra storia e quello che stiamo costruendo attraverso le competenze delle nuove generazioni. Per Deas, questo incontro puÃ² diventare uno dei nuovi fronti della cybersecurity nazionale.

default watermark

â??

economia

webinfo@adnkronos.com (Web Info)

Categoria

1. Comunicati

Tag

1. Ultimora

Data di creazione
Settembre 4, 2026
Autore
redazione