IL PROGETTO BSIMM, LANCIATO DA **Gary McGraw**, CATALOGA E RENDE PUBBLICHE LE PRATICHE COMUNI

Sicurezza OPEN

Le aziende si confrontano sul modo in cui software e servizi sono integrati

Ci sono gruppi di ricercatori universitari, scienziati ed esperti che collaborano da varie parti del mondo, in una cornice open, a uno scopo comune: migliorare la sicurezza informatica delle aziende. Un grande passo avanti in tal senso è venuto nelle ultime settimane, con il lancio delle prime due metodologie ("modelli") open per aumentare la cultura aziendale nel campo della sicurezza. Si chiamano Bsimm (Building security in maturity model) e Samm (Software assurance maturity model). Quest'ultimo nasce dal progetto open source Owasp (Open web application security project), non affiliato a nessuna azienda (vi partecipano esperti e organizzazioni con un libero scambio di idee). «Bsimm e Samm hanno un approccio simile: sono modelli da seguire che dicono alle aziende che cosa sbagliano nelle proprie pratiche di sicurezza e come cominciare a rimediare», spiega Neil MacDonald, analista di Gartner. Questi modelli arrivano adesso, sulla scorta di una riflessione. «L'industria ha capito che il problema non è più nella sicurezza del singolo software o delle reti. Questi aspetti hanno già raggiunto la maturità. Il problema, che ora crea buchi nella sicurezza, è nel modo in cui i software e i servizi sono integrati e usati in azienda», dice Matteo Meucci, alla guida di Owasp Italy (200 iscritti), che il 6 novembre a Milano terrà la conferenza «Owasp Day IV». La risposta di Bsimm e Samm è collaborativa e open, perché sono metodologie pubbliche; chiunque vi può partecipare e le può adottare.

«Per Bsimm abbiamo analizzato, finora, 26 aziende nel mondo, da marzo, tra le quali ci sono nove europee. Anche italiane», dice Gary McGraw, che ha lanciato il progetto Bsimm. Americano, è uno dei maggiori esperti di sicurezza al mondo, su cui ha numerose pubblicazioni. Collabora con i dipartimenti di Computer science delle Università della Virginia e della California.

«Queste aziende (ci sono Google, Microsoft, tra le altre) ci hanno detto quello che fanno per la sicurezza informatica. Abbiamo catalogato così 110 pratiche comuni e le abbiamo rese pubbliche, con Bsimm – continua –. È cosa rara nel mondo informatico che grandi aziende condividano i propri dati. Ma l'hanno fatto, in questo caso, per sapere quello che fanno gli altri», aggiunge.

È il fascino della condivisione: si deve dare per ricevere. «Quasi tutte le aziende, dopo aver visto quello che fanno le altre, hanno aggiornato le proprie policy di sicurezza. A volte, già il giorno dopo». Le aziende scoprono per esempio che le policy altrui, in certi campi della security, sono più convincenti. Oppure di avere, a differenza di altri, ambiti del tutto privi di policy.

La debolezza del modello Bsimm è che misura solo quante e quali policy le aziende adottano; non sa se lo fanno in modo più o meno efficiente. «È vero – ammette McGraw –. Non è un modello perfetto, ma è il migliore disponibile».

«In Italia c'è ancora tanto da lavorare in questo campo, ma alcune aziende ed enti pubblici si stanno muovendo in tempo – aggiunge Meucci –. Perlopiù, però, si limitano a verificare la sicurezza delle applicazioni più importanti ed esposte. Il settore più all'avanguardia è quello bancario e finanziario, ma ora comincia a fare passi avanti anche la pubblica amministrazione. Owasp è in contatto con Consip, il ministero dell'Istruzione e quello dell'Interno». Consip e Owasp, appunto, terranno il 5 novembre a Roma una conferenza sulla sicurezza informatica nella Pa, presso il ministero del Tesoro.

Alessandro Longo

Decalogo aperto

1. Creare consenso all'interno dell'organizzazione
2. Promuovere la cultura della sicurezza all'interno dell'azienda con training informativi
3. Creare policy per far combaciare le necessità normative o le richieste degli utenti con un unico approccio
4. Creare un guida proattiva alla security sulle caratteristiche di sicurezza
5. Guidare l'efficienza/consistenza con l'automazione
6. Costruire competenze interne sulla sicurezza
7. Integrare strumenti all'interno del processo di Quality Assurance
8. Usare tool automatici e review manuali per la revisione del software
9. Dimostrare che anche il codice dell'azienda ha bisogno di aiuto
10. Assicurare che la sicurezza di base delle applicazioni e della rete sia garantita