I.P Serviciul Tehnologia Informației și Securitate Cibernetică

CATEGORII EVENIMENTE CIBERNETICE

	Descriere	Indicatori	Analiză	Remediere
 BRUTE FORCE (ATACURI FORȚĂ BRUTĂ)	Atacatorii încearcă să ghicească parolele prin încercări multiple de diverse parole	Multiple erori de autentificare într-o perioadă scurtă de timp	Log-urile din Active Directory Log-urile aplicațiilor Log-urile Sistemului de operare Contactați utilizatorul dacă îl cunoașteți personal	Blocarea sursei Dacă acțiunile sunt ilegitime blocați contul utilizatorului și investigați suplimentar
 BOTNET	Atacatorii folosesc serverul victimei pentru a executa DDOS atacuri sau alte activități malițioase	Conexiunea la IP-uri suspecte. Trafic în rețea în volum anormal de mare	Traficul de rețea Log-urile OS (analizăm procesele noi) Contactăm deținătorul serverului sau echipa de suport	Dacă e confirmată infectarea, izolați serverul și eliminați toate procesele malițioase. Aplicați patch-uri conform vulnerabilităților identificate
 RANSOMWARE	Un tip de malware ce criptează datele și solicită plată de la utilizatori pentru decriptare	Notificarea de la utilizator Breșa în log-urile AntiVirus Conectarea la IP adrese suspecte	Log-urile conturilor de utilizatori Traficul de rețea Log-urile AV Log-urile Sistemului de Operare	Izolarea stației infectate Solicitarea controalelor AC
 EXFILTRAREA DATELOR	Atacatorii (sau chiar și angajații neinstruiți) exfiltrează date către surse externe	Trafic anormal de intens către soluții de stocare Cloud (Dropbox, Google, Cloud) , Stick-uri USB neutilizate	Traficul de rețea Log-urile Proxy Log-urile Sistemului de Operare	Dacă sursa sunt angajații, contactați managerii și efectuați anchetă internă Dacă amenințarea e externă, izolați stația, întrerupeți accesul acesteia la rețea
 CONTURI COMPROMISE	Atacatorii obțin accesul la un cont de utilizator (prin metode de inginerie socială , furt de date etc.)	Log-uri în afara orelor de lucru obișnuite Schimbări în grupul de conturi Trafic de rețea anormal	Log-urile Active Directory Log-urile Sistemului de Operare Contactați deținătorii de conturi	Dacă se confirmă compromiterea, dezactivați contul, schimbați parolele, efectuați analiza post-incident pentru identificarea modului de compromitere

I.P Serviciul Tehnologia Informației și Securitate Cibernetică

CATEGORII EVENIMENTE CIBERNETICE

	Descriere	Indicatorii	Analiză	Remediere
 DENIAL OF SERVICE (DOS/DDOS)	Atacatorul provoacă interferență în sistem prin exploatarea vulnerabilității DoS sau prin generarea de volum mare de trafic	Trafic de rețea anormal de mare în serviciile publice	Traficul de rețea Log-urile firewall Log-urile Sistemelor de Operare	Dacă atacul DoS e urmare la noi vulnerabilități exploatate aplicați patch-urile necesare, dacă e din traficul de rețea apelați la ISP sau Network support
 ADVENCED PERSISTENT THREATS	Atacatorii obțin accesul la sistem și creează backdoor-uri pentru exploatări ulterioare. De obicei, sunt greu de identificat	Conectarea la IP adrese dubioase Trafic de rețea anormal de intens Log-uri de acces anormale Apariție conturi noi de administratori	Traficul de rețea, Log-urile de acces Log-urile OS (procese noi, conexiuni anormale a utilizatorilor) Contactați server ownerii sau echipa suport	Dacă se confirmă izolați stația afectată, începeți formal analiza și stabiliți un plan de comunicare și post-incident.
 SPAM	Spamul reprezintă trimiterea de mesaje nesolicitate și nepotrivite într-un mod repetitiv și intruziv. Spamul poate fi trimis în masă, sau poate fi targetat .	Mesaje de e-mail în volum destul de mare cu un conținut generic sau nesolicitat și expeditor suspect	Analiza header E-mail sender look-up Filtrele de rețea	Ștergerea mesajelor spam din coada de așteptare a serverului de poștă electronică Blocarea adresei IP a atacatorului
 PHISHING	Atacatorii încearcă să obțină informații confidențiale, cum ar fi parole, date bancare sau informații personale, prin mesaje false sau site-uri web falsificate.	Adresa e-mail suspectă, Conținutul mesajului cu erori text, solicită accesarea link sau completarea/transmiterea datelor sensibile	Analiza header Verificare link Verificare atașamente IP reputation	Ștergerea mesajelor spam din coada de așteptare a serverului de poștă electronică Blocarea adresei IP a atacatorului
 DNS SPOOFING	DNS spoofing implică manipularea serverelor DNS (Domain Name System) pentru a redirecționa traficul către site-uri web false sau malițioase.	Răspunsuri DNS incoerente. Diferențe în IP obținute prin rezolvarea DNS între dispozitivele diferite. Erori "Certificate Mismatch" browser	Traficul de rețea Log-urile de activitate Log-urile firewall	Analiza vulnerabilităților și aplicare patch la necesitate Eliminarea proceselor maliționase