Signs of a Data Breach

Key Indicators Your Organization Might Be Compromised

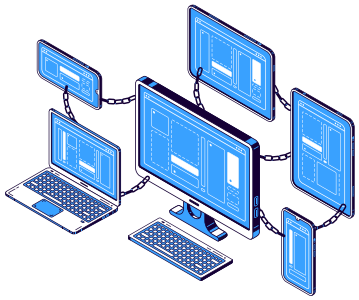
Santosh Kamane

https://www.linkedin.com/in/santoshkamane

1 Unusual Network Traffic:

As part of regular monitoring and vigilance, look out for

- **Unexpected outbound connections (IP address and port) from internal systems**. This could be primary indication of C2C, RAT or remote control by malicious actors.
- **Unexplained traffic spikes or bandwidth consumption** which could be early indicators for DDoS or cryptojacking attacks.
- **Unfamiliar IP addresses or domains in network logs.** Often it could be part of reconnaissance. Keep close watch on the activity.



2 Anomalous System Behavior:

Key indicators to look out for

- **Performance degradation, system crashes, or frequent errors.** Usually this may be reported by end users or application system owners. Do not ignore.
- **Unauthorized changes to configurations or files.** Unless a robust change mgmt and configuration mgmt process is in place, this may be difficult to detect.
- **Unusual processes or services running on systems.** A strong indication of unauthorized malicious access to the system.

3 Abnormal activities in the logs

Most organizations do not make significant efforts to enable critical logging and conduct timely review/analysis for potential breaches.

- **Increased failed login attempts**, especially on critical systems may be indicator for unauthorized access attempts.
- **Unusual logins from unfamiliar locations or outside normal business hours**. Check for these activities or logs from UBA tools.
- Log entries indicating **privilege escalation or unauthorized access attempts.** Monitoring usage of PID is critical tasks and use of these privileged accounts must be reviewed.

4 Unexpected Data transfers

Data exfiltration attempts must be monitored in real time.

- **Unexplained large data transfers** - Check source /destination and identify if its a legitimate activity.
- Unusual file modifications or deletions is again a sign of malicious activity. File integrity controls help track the changes.

5 Alerts from SOC / monitoring tools

What to look for?

- Don't ignore **notifications from intrusion IDS/IPS** systems as it can detect fraudulent activity early.
- **Anti-malware /EDR detecting suspicious or malicious files**. This could be potential sign of malware attack.
- **Firewall / VPN notifications** indicating unauthorized access attempts.

6 Social engineering

Don't ignore social engineering incident reports. It might turn out to be false alerts, but early detection can save you from major data breach.

- **Increased reports of phishing emails,** social engineering attempts such as fake LinkedIn requests.
- Employees falling victim to social engineering attacks.
- Incidents such as data leakage resulting from access to unauthorized print outs or poor data disposal hygeine.

7 Open vulnerabilities in applications & infrastructure

Systems that aren't patched or have reached its end of life - are prime targets for criminals.

- **Unpatched or outdated software with known vulnerabilities**. Check if known vulnerabilities like log4j are remediated.
- **Exploited vulnerabilities** from penetration test reports, if not remediated, could lead to data breaches.

8 External Threat intelligence & staff incident reports

Don't ignore incident reported by external partners or your staff.

- Notifications from third-party security vendors or threat intelligence feeds.
- **Reports from employees, customers, or partners regarding suspicious activities**. Some of these may be false alerts, but could be potential indicator for data breach

9 Web 3.0 / Blockchain based systems.

Web3 / blockchain based systems have unique characteristics

Unauthorized Transactions and smart contract behaviour:

- Sudden or unexpected movement of funds or assets within the blockchain network.
- Unexpected changes to the code or logic of smart contracts without proper notification or approval.

- **Smart contract functions executing differently** than expected or producing unexpected results.
- Multiple failed login attempts or unauthorized access attempts to wallets.:
- Evidence of attempted or successful attacks targeting the blockchain or Web3 system, such as DDoS attacks, 51% attacks, or known vulnerabilities being exploited.

If you are thinking cybersecurity, let's talk to build your robust and resilient cybersecurity program.

WhatsApp business account

Santosh Kamane

https://www.youtube.com/@SecurityAdvisor

https://www.linkedin.com/in/santoshkamane