A Rescue Guide for Hacked SAPs

Your SAP Has Been Hacked?
DON'T PANIC, RESPOND WISELY

VICXER

www.vicxer.com

A TIMELY RESPONSE IS ESSENTIAL.

If your organization is facing an **SAP security incident**, the key to successfully navigate this unpleasant experience is to **respond** in an **expedite** way, without losing focus or panic.

From **Vicxer** team, we would like to share with you, the first actionable actions that we encourage any professional to take after detecting a **cyber-attack** against your **SAP ecosystem.**

While facing an **SAP security incident**, it is **critical** to the success of the upcoming investigation, that you manage to **safeguard all the logs** from the different SAP layers, and to capture the **SAP configurations** that regulates the behavior of the **SAP audit trails.**

To help you tackle this endeavor,
Vicxer team summarized a set of logs and configurations that **must be verified** and **safeguarded** for future analysis:

Log	Default Location	Configuration To Review
ABAP Security Audit Log	/usr/sap/<SID>/<instance>/log/audit_instance_number	SAP Parameters *rsau/enable, rsau/local/file, rsau/max_diskspace_local, rsau/selection_slots, rsau/max_diskspace/per_file*
SAP Gateway Log	/usr/sap/<SID>/<instanceFolder>/work/	SAP Parameters *gw/logging, gw/acl_mode, gw/acl_file, gw/sec_info, gw/reg_info*
SAP ICM	/usr/sap/<SID>/<instanceFolder>/work/	SAP Parameters *icm/security_log,* icm/HTTP/logging_client_<xx>
SAP Java (HTTP)	/usr/sap/<SID>/<instance_name>/j2ee/cluster/server<number>/log/ /usr/sap/<SID>/<instance_name>/j2ee/cluster/server<number>/log/system	NA
SAP Message Server Audit Log	/usr/sap/<SID>/<CentralInstanceFolder>/work/	SAP Parameters *ms/audit,* ms/conn_timeout

Log	Default Location	Configuration To Review
SAP Web Message Server	/usr/sap/<SID>/<CentralInstanceFolder>/work/	SAP Parameters ms/http_logging, ms/HTTP/logging_0
SAP Enqueue Server	/usr/sap/<SID>/<CentralInstanceFolder>/work/ /usr/sap/<SID>/<instanceFolder>/work/	SAP Parameters enque/logging, enque/log_file
SAP Hana	/usr/sap/*<sid>*/*<instance>*/*<host>*/trace/*.ltc /usr/sap/*<sid>*/HDB*<instance>*/exe/hdbtracediag /usr/sap/<sid>/SYS/global/hdb/custom/config/global.ini /usr/sap/<sid>/HDB<inst>/<host>/nameserver.ini /usr/sap/<sid>/HDB<inst>/<host>/global.ini /usr/sap/<sid>/SYS/global/hdb/custom/config/nameserver.ini	Audit Views: CAUDIT_LOG, XSA_AUDIT_LOG or its union ALL_AUDIT_LOG Configuration Files: Capture all the mentioned ini files
Other SAP Databases (MSSQL, Oracle, etc) Log	Please refer to the vendor's documentation	Please refer to the vendor's documentation
Operating System Audit Log	Please refer to the vendor's documentation	Please refer to the vendor's documentation

AS AN ALTERNATIVE AND WHENEVER POSSIBLE,

CONSIDER TAKING A SNAPSHOT OF THE AFFECTED VIRTUAL MACHINES.

AND WHAT NOW?

While your team diligently safeguards logs and documents the current SAP configurations.

Don't hesitate to reach out to our dedicated

CYBERSECURITY INCIDENT HOTLINE.

CALL US AT
+1-(857)-242-9700

- **WHAT WILL YOU RECEIVE?**

Expert Guidance

Our consulting team is here to navigate you through these challenging times, providing step-by-step instructions and strategic advice tailored to your specific situation.

Flexible Services

You have full control over when and how our consulting services are delivered. Whether you need immediate intervention or scheduled support, we adapt to your needs.

Personalized Support

Enjoy the human touch with a dedicated consultant who will be your go-to expert, ready to assist whenever you need them most, ensuring you have a trusted advisor by your side.

Ready to enhance your SAP security?

Take your next steps

- Connect with us
- Explore our technical resources
- Talk with an Expert
- Request a free Consultation

Vicxer is a leader in **ERP cybersecurity** solutions for **SAP**. Armed with 15+ years of experience, the Vicxer team has been working with Fortune-500 companies, governments, and NPOs across the world. **The Vicxer Platform** delivers a comprehensive set of cybersecurity solutions for SAP, including vulnerability management, compliance assurance, and continuous monitoring for SAP environments.

Vicxer is headquartered in Miami, Florida, with offices in Lisbon, Portugal, and Buenos Aires, Argentina. We are also present in major cities around the world through our extensive network of over 20 partners.

For more information, connect with Vicxer on LinkedIn, Mail or visit https://www.vicxer.com.