Alcea Tracking Solutions
Data Breach Action Plan

Public Document

Contents

Summary

The intent of this document is to be proactive and outline an action plan which will allow Alcea Technologies Inc. to respond to a data breach or attack to its hosted environments. This action plan will aim to minimize any loss of data and any additional damage from a such an event.

Alcea has operated a hosted environment for over 10 year and has never had a security breach. However, we realize that technology is changing every day and that security is an ongoing process which must be studied and continually addressed.

Organizational Layers

There are three separate organizational layers which must be identified separately in our ATS hosted environment. Precautions must be identified at each layer:

IBM Softlayer (Bluemix) Infrastructure – we have researched and used multiple vendors for hosting ATS servers in the past. The IBM Softlayer infrastructure was chosen for the following reasons:

- Reputation – IBM has a longstanding reputation in the computer industry. IBM acquired a global data center called Softlayer and has established itself as a major supplier in this industry.
- Compliance – IBM meets major industry guidelines and has audit documentation to prove it: https://www.ibm.com/cloud-computing/bluemix/compliance
- Support – IBM has a proven support record. Alcea has hosted its servers with Softlayer for the last three years and receives excellent support from the IBM support staff and its affiliates.
- Backups – Alcea has aligned itself with SimpleBi (an IBM affiliate) to provide a third party backup platform, using R1Soft Backup Manager.

Alcea Tracking Solutions software and maintenance

- Alcea is a small company with very little turnover. All existing employees have been employed with Alcea for 6 or more years and possess government of Canada Secret clearance qualificatons.
- Alcea Technologies uses a standalone product which has proven itself to be a leader in collaborative tracking software over the last 15 years. The requirements for this software are extremely small and help limit exposure.
- Systems are hosted on the linux platform which is one of the safest environments to secure.

Customer use and maintenance

- The ATS software provides multiple security options to help safeguard access to the ATS system. Customers must be made aware of the security options in the ATS server configuration.
- System Configuration – ATS is a configurable system which allows a customer to define security groups and access levels based on company permissions and organizational structure. Administrator training is highly encouraged to limit inappropriate access to data due to configuration errors. Alcea provides excellent support packages to help with any customer inquiries.
- Each customer must keep Alcea informed about system contacts so that any desired changes to the system or updates are properly communicated.

Safeguards

- Minimal Configuration – ATS hosted servers run a very minimal Linux configuration with a standard documented configuration.
- Limited Access – Access to any ATS hosted server is limited to technical staff at Alcea Technologies Inc, all of whom possess Government of Canada secret clearance.
- Server updates – regular server updates are made to all ATS servers. In addition, systems are moved to newer Linux distributions when needed, rather than being updated.
- Logs – All traffic to servers and ATS instances are logged
- Server Firewalls – port traffic from servers is limited to ports listed above
- Monitoring – Alcea runs a Nagios server for continuous reporting of server availability, disk requirements and instance availability. Availability of each server is also monitored as part of the Softlayer network.

Detection

The detection of an intrusion can be hard to identify, so Alcea takes a hard approach to any of the following suspicious events:

Suspicious logs – A number of logs are available for auditing on any hosted system:

- Server logs are located in /var/log/syslog, documenting information about the server such as restarts, logins, email traffic. Auth.log documents all logins and attempts with the originating IP. If suspicious messages occur, simple changes to the hosts.allow/hosts.deny can limit access to the machine to specific IP addresses.
- All access to each Alcea product is passed through apache process and logs are provided in /var/log/apache or /var/log/httpd
- ATS logs are located in logs directory of each hosted instance. Suspicious changes to a system can be tracked and monitored through these log files. This includes logins, failed logins and administrative changes.

Abnormal Behaviour

- Except.log/nohup.out exists for each ATS instance monitoring abnormal messages from the system such as suspicious file requests and abnormal exceptions.
- All ATS records provide a full historical traceback to identify who and when changes are made to data records.
- Backups exist for up to 4 weeks to identify missing files

Abnormal processes

The following ports are required on a general ATS system:
80/443 – Apache2
22 – SSH connections to server
48007/48008 – Softlayer monitoring
1167 – connections to backup server from r1soft
25 – email notification (SMTP)
Any other ports should be associated with a ATS instance for internal apache forwarding only.

The "netstat -an" command will identify any additional ports that are currently being used. Any such ports must match an associate ATS system on that server or they may identify an unknown process.

Warnings

- File changes or missing files
- Warnings from external parties such as return email messages, third party complaints of excess traffic.
- Customer complaints – customers identify data that has been stolen or viewed without permissions.

If any of the above examples exist comparisons can be made to backups and an investigation must be conducted.

Action Plan

Identify Current Breach

If a breach is suspected or identified, an immediate lock down of suspected machine(s) must be performed. The lockdown will include password changes to the suspected machine and changes to the hosts.allow/deny files to limit all traffic to machine.
The lockdown will include discussions with the contacts for all hosted clients on the suspected machines.

Evaluate Remedy

An immediate quick evaluation of the impact of the breach will be made to determine if the customer would like to move their data to a new machine for immediate relief. Every attempt will be made to restore the service back to the customer, once they are happy with our response to the problem.

If the breach was confirmed, a new machine will need to be instanced and configured to ensure there are no undetected vulnerabilities exist on that node.

Investigation

After the new machine is set up, a careful assessment of the old machine will begin to identify source of the breach and incident timeline. This may include an external party if needed. Careful inspection of all log files will begin. An inquiry will be made to each customer on the machine to investigate their unique configuration.

Changes to safeguards and policies will be discussed and documented. When a full explanation is available, it will be given to the customer.

Propogate Updates

Any suspected breach will involve password changes to all servers in the ATS hosted infrastructure. Results of the investigation will determine what steps need to be taken to protect the infrastructure going forward.