PRIVACY IMPACT ASSESSMENT OF CARBON BLACK PROTECTION AND CARBON BLACK DEFENSE

Executive summary

The produced paper acts as the PIA (Privacy Impact Assessment) conducted over the selected Carbon Black Products. The products in consideration are CB Protection and the CB Defense. It has been observed that some of the focal apprehensions and the potential privacy concerns have been specifically paid utmost attention. The paper would be comprised of the analysis of pertinent risks for the selected products. The service provided by Carbon Black provides a parental control for locking the servers along with managing the critical systems. The CB defense is a solution that combines antivirus along with detecting and responding endpoint for presenting a lightweight solution for managing the system.

Table of Contents

Introduction

The Privacy Impact Assessment is being conducted for understanding the policy of Carbon Black, specifically for CB Protection and CB Defense. PIA is developed for determining the risk along with underlining the effects of the risks. A PIA helps in ensuring the policy requirements, applicable legal as well as regulatory requirements for privacy are agreed. PIA helps in evaluating the process for protection along mitigating the potential risks related to privacy. The assessment of the impact of the policy for Carbon Black will help the company to reduce the expenses on privacy mistakes along with enriching the process of making informed decisions. Reducing privacy risk helps in gaining the trust and confidence of the public.

What information is being collected?

Carbon Black collects data from the consumers through services such as CB defense and CB protection in the form of metadata. The metadata mainly consists of the way a device is being used, data about the software application, record of login, details of executed files along with processes that are launched. Carbon Black collects the types of operating system used in a system. The personal data, including the IP address and device name, are registered in the company record that is used for identifying the risk in privacy[1]. The information such as the full name of the user or the organization name authenticated telephone number, valid and accessible email id, residential address are collected through the web portals that are used for planning the risk assessment plan. The information, including the details about the equipment, browsing pattern, cookies, tracking code along with user data, is collected for managing the policy of Carbon Black.

[1] [1] *Harvesting Cb Response Data Leaks for fun and profit | DirectDefense*. (2017). *DirectDefense*. Retrieved 16 October 2019, from https://www.directdefense.com/harvesting-cb-response-data-leaks-fun-profit/

Why is the information being collected?

The information is collected for the following reasons:

- To improve the product as well as service along with providing, operating, securing and personalizing the services.
- To ensure that the response system responds to the new threat along with developing features for enhancing the response towards privacy issues.
- To conduct research along with analyzing the present system as well as participating in the threat intelligence network.
- For sending out information about the product to the customers and informing them about the changes in the policy.
- To provide support to the customers that include controlling the customer account, coordinating with the vendors along with responding to the queries and comments raised by the users.
- To provide protection against fraud claims, criminal activity, and complying with regulatory policies.
- To complete the activities those are in accordance with the privacy policy along with those raised by the customers.
- To plan as well as take action for protecting the rights and property of the Carbon Black
- To monitor and protect the system from unauthorized use of system along with the services of Carbon Black.
- To protect the websites along with web portals from all unauthorized misuses.
- To initiate action against the subpoena along with discovery pursuant against the federal law.

What is the intended use of the information?

The main intended use of the collected information is to organize the privacy process along with ensuring that the users of the services provided by Carbon Black are able to access their services. The organization uses the collected information to help users have a continue authenticated access to their accounts along with tracking their work for identifying any unauthorized activity[2]. The collected data are used for providing the customer data to the customers who have lost access to their account or been locked. The useful keys such as cloud keys, communication infrastructure, keys for the app store, key for proper sign-in are provided by using collected data after verifying the authentication.

With whom will the information be shared?

The business organization, Carbon Black might share the information of the customers with third parties including agents, business partners, service providers and partners. The company shares the information under proper safeguards, which ensure no further leaking of the confidential personal information of the customers. However, the company comply with the EU-US privacy shield and does not share any information on the users belonging to the European Union. The business organization has a privacy shield that ensures data integrity, access, security, choice, along with liability and enforcement. The company doesn't retain information of children who are aged less than 13 years. The company immediately deletes the information provided by users who are under 13 years of age.

[2] *Privacy Policy | Carbon Black*. (2019). *Carbon Black*. Retrieved 16 October 2019, from https://www.carbonblack.com/privacy-policy/

What opportunities do individuals or businesses have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information and how can they grant such consent?

The individuals, along with business, have little opportunities to decline to provide information as the provision of providing information is voluntary. However, provided by users are used for providing support along with stopping all unauthorized access and use of service provided to the users. The company will not be able to provide full support to the customers who decline to provide their personal information[3]. The company has a privacy shield for providing maximum privacy of the detailed information provided by the users. The company does not force the customers to give any information along with not collecting any data from the users aged less than 13 years.

How will the information be secured?

The CB protection has strong security for the critical system along with the data centres. The CB protection follows the lockdown system, continuous compliance and high performance and low touch. The lockdown system stops all attacks, both malware as well as non-malware by stopping all unwanted changes[4]. The lockdown system is basically used to stop file-based attacks, memory-based attacks, next-gen attacks using the obfuscated malware and script-based techniques such as PowerShell. The continuous compliance helps in complying standards of the major regulators[5]. The continuous compliance regularly monitors the assets of the user along with tracking the policies for change and control, calculating all drift from the baseline specified

[3] *CB Defense Datasheet | Carbon Black*. (2019). *Carbon Black*. Retrieved 16 October 2019, from https://www.carbonblack.com/resource/cb-defense-datasheet/
[4] *CB Protection | Application Control Solution | Carbon Black*. (2019). *Carbon Black*. Retrieved 16 October 2019, from https://www.carbonblack.com/products/cb-protection/
[5] *CB Defense | Next-Generation Antivirus | Carbon Black*. (2019). *Carbon Black*. Retrieved 16 October 2019, from https://www.carbonblack.com/products/cb-defense/

by the user. The CB protection helps in providing integrity to the configuration of the deployment of a business organization along with continuous monitoring and reporting the implemented privacy policies. The high performance and low touch application ensure that the protection process is easy and uses the cloud-driven along with IT trust for automatic approval[6]. The CB protection helps in blocking files having risk on the system along with analyzing new files before allowing it to the system. The use of CB protection and CB defense ensure high privacy of the information stored by monitoring the latest files, drift in the baseline.

Risk Assessment

The risks identified in CB protection include:

- Monitoring all files and prevents deletion: the CB protection monitors all file however, does not stop deleting files. The collected data might be deleted and it is not possible to identify or recover deleted files in the monitoring process.
- Autotrust IT staff software: The IT staff systems are untrusted, which might increase risk. The malware might be transferred to input on the system through the untrusted IT staff system.

The risks identified in CB defense include:

- Monitoring all data on endpoints and accessibility to all employees: The files are a monitor at the endpoint in CB defense that raises chances for introducing malware and stealing data within the process. All employees have accessibility to the data that increases the chance of tampering privacy.

[6] *CB Protection Datasheet | Carbon Black*. (2019). *Carbon Black*. Retrieved 16 October 2019, from https://www.carbonblack.com/resource/cb-protection-datasheet/

- Give alerts about risky behavior: the CB defense does give strong alerts about the risky behavior along with a shift in the specified baseline. The risky behavior indicates the chances along with scope for disturbance in privacy protection.

Recommendation

The recommendations for Acme Dynamics implementing the product of Carbon Black in Europe are:

- The company should be aware of the type of data existing with their system, which are used by the agents from Carbon Black solution.
- The business organization needs to understand the types of data collected along with tea places in which the Carbon Black Company intend to use the data.
- The business enterprise might appoint analyst who have access to the multi-scanner that works based on cloud and identify the data which might pertain to the business organization.
- The company might disable the cloud upload option if they have an option to do so.

Conclusion

Carbon Black Company has several products however, two main products are CB Defense and CB Protection that provide security and privacy to their customers. The policy impact assessment indicates that the services provided by Carbon Black are highly efficient and can be used by organizations such as Acme Dynamics. The assessment of the impact of the policy of Carbon Balck organization helps in concluding recommendation that needs to be followed while implementing services of carbon black along with maintaining high privacy.