BizzSecure
PEACE OF MIND FOR InfoSec

How to Manage Application Security Risks

Table of Contents

Introduction

The digital world runs on applications. These useful nuggets of software could be on your phone, tablet, computer, or controlling major business operations of organizations around the world. The evolving usage of applications has added data handling among their many functions. Data handling could include anything from obtaining or generating customer or employee data to sharing or processing it. Now, when applications are being used by organizations to conduct their data-related business operations, it is also important to keep the data assets secure so that they are not lost or misused.

While it is important to secure the network over which these applications are downloaded, used or shared, it is also necessary to individually protect each of the applications you use. This is even more important in the current age when hackers and intruders have decided to target individual applications in addition to the networks that carry them. Compromised applications can be prone to intrusion, data leakage, and subsequent misuse of data by the intruders.

Application security measures must be incorporated at all three stages in the lifecycle of an application: (1) the development stage, (2) the revision stage, and (3) the post-marketing or post-deployment stage. This does not mean that the task of ensuring application security ends with these measures. Application security risk management is an operation that must be carried out throughout the lifespan of your organization.

Management of application security risks entails a series of important steps, two of the primary ones being application security risk assessment and application security risk remediation. Risk assessment helps you identify the risks associated with all the applications being used in your organization. On the other hand, risk remediation involves the elimination of these application security risks so that they do not breach your applications again.

In this book, we have discussed each of these major steps that help manage application security risks. We start with different kinds of application security risks. We further discuss the steps that organizations must take to conduct an application security risk assessment, followed by remediation. Additionally, to make application security management more effective, we have discussed the integration of application security risks with remediation. In the end, we have also described an automated, all-in-one platform created by BizzSecure to help you manage all your application security risks – the EAID solution.Let’s get started.

Application Security Risks in an Organization

Before we delve deeper into how to manage application security risks in your organization, we must first understand the common types of risks that applications bring with them to any organization. Since the modes, devices, and reasons for accessing applications have changed and grown over the last few years, the kinds of application security risks have also evolved.

Here are some of the major application security risks that organizations must protect themselves from on a daily basis:

Virtual Private Networks or VPNs

Some organizations tend to assume that since they are providing a VPN for their employees to access all their business applications, they do not have to worry about application security. This is a dangerous assumption. In fact, VPNs often tend to skip and go around some of the basic data security systems to provide access to different applications. This makes your applications highly vulnerable to intrusion, hacking, and malicious unauthorized access.

Public cloud environments

We have already established that some of the most important risks that applications face these days are due to unauthorized access by malicious actors. However, this risk is not limited to VPNs. Expectedly, public clouds that are often used to store or access these applications greatly increase the risk of unauthorized access, too. They do not allow for separate security measures for each user, which makes the applications extremely vulnerable.

Third-party vendors

Third-party vendors, old or new, present the greatest risks to application security. You do not have any visibility into the development process of the applications supplied to you by third-party vendors. Therefore, you cannot be sure if they follow information security policies and regulations to the same extent as you do. You also cannot be sure of the vulnerabilities of the different applications that you have procured from these third-party vendors. Moreover, new third-party vendors provide their own application security modules. These may not necessarily be trustworthy. When managing application security risks, third-party vendors must get a high priority.

Unique blocks of code

Applications become distinct from others of their kind through specific blocks of code that are unique to them. Hackers tend to target these unique blocks of code as they give them the means to overcome the typically used application security measures. Moreover, if the applications you are using have not been developed in-house, it is going to be almost impossible for you to change these unique blocks of code that make your business applications vulnerable. Therefore, the unique blocks of application codes pose great risks to your organization’s application security posture.

Authentication

We keep talking about unauthorized access to applications because it is a critical issue when it comes to applications. However, how does one ensure that a person or entity accessing an application is authorized? This requires a set means to authenticate the identity of the user. Different ways of authentication currently exist, such as password protection, security answers, captcha, one-time passwords, two-factor authentication, etc. Unfortunately, if your applications use inefficient authentication measures, authentication is going to do more harm than good. It can put your applications to an even greater risk of intrusion, making it an important risk factor to consider in application security risk management.

The points discussed above describe only some of the risk factors associated with applications. The purpose of the sections in the rest of this book are to help your organization manage these and all other application security risks that endanger your data assets. In the next section, we start with the first step in the application security risk management work plan – risk assessment.

Application Security Risk Assessment

You may have developed applications for your business purposes in your own organization or leased or purchased applications from third-party vendors. These applications could be used for obtaining new customer or employee data as well as for storing, processing, or sharing old and new data. Clearly, any kind of data breach in your applications can be extremely harmful to your organization's data assets and business continuity. Therefore, application security management is an essential component of any organization's information security framework. Like other security management workflows, application security also requires that a thorough application security risk assessment be conducted first.

Here are some steps you should follow to perform application security risk assessment in your organization:

Survey all the applications used in your organization

The first thing you need to do while performing application security risk assessment is to create a list of all the applications being used in your organization for handling data in any manner. All surveyed applications should be divided into categories based on their usage statistics, the kind of data they handle, and the impact of using those specific applications on your business operations.

Identify the risks associated with each application

We have already discussed the various kinds of application security risks that your organization may be exposed to on a daily basis. One of the most important steps of application security risk assessment is to identify the risks associated with each and every application that is used in your organization. Based on the risks identified, these applications must be categorized into 'high risk,' 'medium risk,' 'low risk,' and 'no risk' applications. 'High risk' applications are those that are the most vulnerable to an application security breach. Vulnerability will be affected by two main factors: (1) the kind of data being handled through that application – financial information, healthcare-related data etc. and (2) the strength and integrity of the current application security measures in your organization that help in relation to the risk of interest.

Learn from past instances of application security breaches

If for some unfortunate reason, one or more of your applications have been compromised in the past, you can use this experience to identify and fill the gaps in your application security strategy. A thorough analysis of your past application security failures will help you identify new vulnerabilities to your organization, thus contributing to the protection of your sensitive data assets in the future.

Check for compliance-related issues

Are your employees, customers, and third-party vendors compliant with the application security policies set forth by your organization? This is an important question that all application security risk assessments aim to answer. Categorize your apps as compliant or non-compliant based on the current usage in your organization.

Design an informed application security plan

Using your application risk assessment to develop or update your security plan of an updated and more robust application security strategy, is an important step that must be incorporated in the application security risk assessment itself. Think of what all you can do to enhance application security in your organization – going back to the source code of in-house applications to modify the vulnerable coding blocks, changing the third-party vendors whose applications you have been using, adding more layers of authentication to grant access to applications, and other such steps.

Application risk assessment is a must-do task in application security risk management. Follow the steps that we have described above and get started with application security risk management in your organization. In the next section, we discuss a technology that is both a boon and a bane to application security.

Container Security

So far, we have discussed what application security risks are, and how they can be assessed. Now, before we discuss how you can keep your organization's applications secure by remediating any risks in the event of a breach, we want to shed some light on a relatively new technology that has been designed and is being used to secure your applications. Unfortunately, this technology is also the newest victim of the intrusion by cybercriminals. We are referring to container technology.

Container technology is gaining traction among all application developers these days. It is an application virtualization technology that can help you develop as well as market your applications. Containers allow for a variety of applications to be stored together such that they can run on the same operating system kernel while still being isolated from each other. This makes the applications more portable and easier-to-use. Additionally, this has also led to application developers making use of container technology to keep applications more secure.

Therefore, containers have become a way to secure your organization's applications as well as a new target for hackers and cyber intruders. This makes it extremely important to make container security an integral part of application security management.

Here are some steps you should follow to improve container security in your organization:

Integrate container security with other forms of information security

When we talk about information security, we include network security, physical security, vendor security, as well as application security. Similarly, in this age, we must also include container security as another crucial information security subdomain. Since application security is often already linked with the information security infrastructure in organizations, integrating container security in your current security policies will be easy.

Ensure the trustworthiness of container image sources

Containers are made up of multiple different layers of code or files, each of which is known as a container image. Container images can greatly impact the security of your containers, and hence, your applications. When your organization is developing in-house applications using container technology, do not forget to ensure that the container images used to create the container are downloaded, purchased, or shared through trustworthy sources or vendors. If you can trust the container image sources, your application security risk management plan takes several leaps forward.

Improve visibility

Just like websites and applications, all containers also need to be hosted somewhere. Your applications' container(s) may either be hosted at a server located in your organization or even in a cloud environment that enables remote access. Ensuring application and container security requires proper visibility of your containers and their host environments, wherever they may be located. Visibility of all the container images and their sources is also important to ensure that you are able to conduct a thorough and complete application security risk assessment for your organization.

Update all container-related frameworks

Just like updating your applications is necessary to keep up with cybersecurity, it is also important that you keep updating your containers' operating system kernels and important container images or layers to improve your container and application security framework. In particular, if you update your container's host operating system to one that can increase the container's isolation, you can greatly boost container and application security in your organization.

Keep an eye on who gains access to your container images

Once again, this step is important for organizations that develop their own applications and containers. We have already emphasized how important it is to obtain your container images from the best and the most trusted sources. However, once you have downloaded the required container images from these trusted sources, it is up to you to monitor who gains access to them. Even if you develop your own container images, it is important that you keep an eye on who is able to access these. Secure all your container images to ultimately increase the security of your containers and applications.

As we have mentioned before, while containers have presented a new way of securing your applications, they have also become a new vulnerability to be aware of in any organization that handles digital data. An important way for organizations to manage their application security risks is to actively pursue the security of their application containers. Follow the steps we have described in this section to ward off all the application security risks related to container technology. In the next section, we discuss some more ways to deal with application security risks that may have breached your organization.

Remediation of Application Security Risks

Now that we have discussed application security risks, their assessment, and important technology that tries to keep them at bay, it is time for us to look at how these risks can be eliminated in case their threat becomes live.

Remediation is your ultimate weapon to eliminate all the application security risks in your organization. Here are some ways in which you can remediate the application security risks pertinent to your organization.

Change the ways in which you grant application access to your users

One of the first things that come to mind when thinking of any kind of information security risks is unauthorized entry into your data stores. Unauthorized access to your organization's applications leads the intruders to sensitive customer information that they can then misuse. In doing so, these intruders not only steal valuable data from your organization but also risk your organization's business continuity.

An obvious way to deal with unauthorized access is to change and upgrade the ways in which you grant access to application users in your organization. If your applications are only password-protected right now, consider using a two-factor authentication system. Perhaps you could also include a captcha as part of the access authorization process. Think of these new and more secure ways to restrict access to your applications and thus, to your data assets.

Modify the source code

Some hackers target the unique blocks of codes present in the application. If you are able to identify these vulnerable sections in the codes of the applications that are designed within your organization, consider modifying them and making them more robust. This will greatly reduce the overall vulnerability of your applications.

To make remediation easier, you can even consider modifying the source code immediately after you identify new risks after you have launched the application. This is because many risks present themselves only when the application is in use. Identifying and remediating such risks sooner will nip these issues in the bud as well as help in a smoother and much safer use of your applications.

Ensure that your employees and vendors are compliant with risk management plans

Application security does not only depend on the technological measures being taken to secure your application-based data from intruders. It also depends heavily on whether or not your employees and third-party vendors follow the application security policies laid out for your organization. Non-compliance renders any security policy ineffective and meaningless.

You must ensure that both your employees and vendors are compliant with the application security measures in your organization. These could be relatively simple measures such as making all applications password-protected, or they could be some more involved measures such as encrypting all application data. If you use your applications to handle any sensitive data that is

regulated by federal or state laws or industry standards, make sure that the applications as well as the vendors that provide them strictly abide by these laws. In such cases, non-compliance could not only cost you a lot of money but also your reputation, your customers, and even the license to operate your business.

It is important to keep learning

Applications represent the rapidly changing technology of the modern age. As the underlying software that helps you run your business operations changes, so do the risks that endanger it. Therefore, it is important to keep up with the changes in both the application world and the world of cybercrime. To do this, you must engage your IT and information security teams.

What are some new strategies that you could use to secure your applications? Could you incorporate some changes at the coding level to make your applications safer? Are there new vendors that provide novel security measures incorporated in their applications? Answer these and other such questions as part of your risk remediation process.

Ensure container security

We have already discussed container security in detail in the previous section. We also talked about the ways in which you can improve container security in your organization. Here, we reiterate this point because it is just so important in the current age. When an application security risk presents itself, go back to your assessment of container risks in your organizations and check if container risks could be the cause for the application breach. If so, you must focus on the sources of your container images and ensure that the images are safe to use as layers for your containers.

Also, check if you need to modify the host operating systems that you have been using for your containers. As we have mentioned before, operating systems that ensure the highest level of segregation or isolation between the different applications in a container are the best for security purposes. Taking such measures will help you remediate all container-related application security risks in your organization.

Follow the steps that we have described in this section to remediate some of the most common application security risks that any organization faces. In the upcoming section, we describe the need and the means of integrating your organization’s application security risks with their corresponding remediation measures.

Integrating Application Security Risks with Remediation

So far, we have discussed application security risks, their assessments, and the corresponding risk remediation strategies separately. However, in a continuous application security workflow, these three aspects cannot be kept segregated from each other. On the contrary, they must be integrated completely with each other so that the application security framework is robust and actionable.

Your organization may be using a number of different applications to carry out its business operations. Whether these applications were developed in-house or either purchased/leased from other vendors is immaterial to the need for application security in any organization. It is the use of these applications to handle sensitive data obtained from customers or employees that makes it necessary to implement thorough application security measures.

Here are some ways in which you can integrate application security risks with remediation in your organization.

Start with the integration of vendor risks

Application security risks are closely linked with the security risks posed by the vendors that make them. Therefore, in order to integrate application security risks with remediation, it is important to first integrate third-party vendor risks with remediation in your organization.

Integrate container security risks with the information security workflow

As we have discussed earlier in this book, container security has become an integral aspect of application security these days. Since containers are being used as a means to promote application security, they have also become potential victims for cybercriminals. Therefore, an important part of integrating application security risks with remediation is to integrate container security risks with your current information security management work plan.

In-house applications should be integrated into the development stage

Many organizations have capable, trained IT teams that develop applications for their regular business use. Such organizations must take application security measures in the application's development stage itself. All newly developed applications should be promptly screened to detect any vulnerabilities that were not predicted in the coding stage. Applications must also be screened for risk vulnerability after they have been launched for use. All identified application security risks should also be linked to their corresponding remediation measures in this development stage. This will serve as an important step towards integrating all application security risks with remediation in your organization.

Secure the unique sections in the code of your applications

All applications have some unique sections or blocks of codes that make them distinct from other similar applications. These unique blocks of code are typically targeted by hackers to breach your application security barrier. Therefore, it is important to secure these vulnerable sections of the code to secure your entire application. Think of how you can remediate the risks arising from these

vulnerable coding blocks when your IT team is in the coding stage. This will ease the integration of application security risks with remediation in your organization.

Automate the application security workflow

Automation is the key to improving any security management workflow. Manual application risk management can be tedious and error-prone. Therefore, it is truly beneficial to use software that provides a platform to easily list out and prioritize all the applications that are in use in your organization. You can rank and visualize them in the order of the risks they pose. Application risk management features such as container security management and third-party vendor risk management can be incorporated within such automated platforms too. Moreover, automation also allows you to link appropriate remediation measures with each of the application security risks identified above. This way, application security risks, assessment and remediation all become part of the same software portal. BizzSecure's EAID solution provides a robust way to automate the application security workflow in your organization. In the next section, we will discuss the EAID solution and the ways in which it makes application security management simpler, prompter and better.

Overall, the growing security concerns associated with applications have made it critical to integrate application security risks with remediation in any organization. You can make the integration process easier for your organization by following the steps described in this section.

Managing Application Security Risks with BizzSecure's EAID Solution

Throughout this book, we have discussed the several steps that make up an application security risk management plan – from risk assessment to risk remediation. Given the various steps involved, managing application security risks might seem like a daunting task. The experts at BizzSecure understand both the importance and the tediousness of following a thorough application security risk management program. Therefore, they came up with the Enterprise Assessment and InfoSec Design (EAID) solution to manage all information security risks in an organization. Application security risks are also managed easily through this all-in-one platform.

Let us take a look at what all the EAID solution can do to make the management of application security risks easier.

It automates application security risk management

The first and foremost advantage of using the EAID solution to manage your application security risks is that it is automatic. All the steps in application management – from risk assessment to risk remediation and reassessment – are easily performed through the EAID solution. This removes the tediousness of all these tasks in the workflow. Ultimately, it helps save not only time but also financial and human resources in your organization.

It integrates application security risks with remediation

We dedicated the entire previous section of this book to discussing the importance of integrating application security risks with remediation, and the ways to achieve it. Think of the EAID solution like the crux of that section. It allows you to easily integrate risks and remediation across locations, departments, and risk types – all on one platform.

It helps you generate risk reports

Quite often, the analysis and interpretation of the results of a risk assessment or remediation assessment present the biggest challenges to the information security department. This is because the results need to be compiled in a meaningful and technical manner that is also understandable to the non-experts in the field of information security. The EAID solution helps you generate such reports on your application security risks, remediation, and compliance. You can generate these reports for all your departments and all the physical locations of your business operations. You can also immediately export and share the risk reports with all the concerned stakeholders in your organization.

It provides an efficient way to prioritize application security risks

You might remember from the 'Application Security Risk Assessment' section of this book that it is important to identify and prioritize all the application security risks in your organization. We had suggested that all risks be categorized into 'high risk,' 'medium risk,' 'low risk,' and 'no risk' categories (or other similar classes). The EAID solution provides an easy way to achieve this classification. It lets you assign weights to all the application security (and other) risks that you identify during your survey of the risks in your organization. These weights will be based on your

analysis of the vulnerability of your data assets and applications to the various risks, as well as the general potency of those risks. Once you assign weights to all the risks, they immediately get ranked, thereby highlighting your application security priorities.

It increases the visibility of risks for each application

Visibility of all application security risks is important to accurately guide your remediation efforts and to redesign your application security policies in an efficient manner. All the concerned people in your organization – executives, information security teams, application developers – can be authorized to access the EAID solution in your organization. All these stakeholders will then be able to continuously monitor the application security risks in your organization as well as any ongoing remediation efforts. Risks and remediation can be separately identified for each individual application being used in your organization. Therefore, the EAID solution greatly improves the visibility of all application security risks.

It makes resource allocation more transparent and efficient

The various steps in application security management require resources – both financial and human. The EAID solution increases the visibility of all available financial and human resources in your organization. You can easily allocate these resources for a given task in the application security management work plan. It will also let you look back at previous allocations to help you understand if any changes in resource allocation are required.

It lets you assess compliance and security maturity

As we have mentioned earlier in this book, application security policies must be complied with in order for them to be effective. The EAID solution lets you assess the compliance levels in your organization. It provides a set of questionnaires to be filled out by authorized personnel. These questionnaires include all the information security policies – including those that deal with application security – in your organization. Authorized users can fill out the questionnaires and provide evidence for their answers pertaining to the health of your organization's security posture as well as compliance. you can also compare the results of such assessments with the results from any previous assessments in your organization. This way, the EAID solution allows you to assess compliance within your organization. It also lets you analyze how application security and other forms of information security in your organization have matured over several years.

Given the several benefits of the EAID solution to your organization's application security and overall security posture, consider subscribing to manage the application security risks in your organization.

Conclusion

Applications have become indispensable in today's digital age of information. They have become prominent players in data handling across multiple industries. As a result, hackers and cybercriminals take advantage of the necessity of these applications. They are continuously creating new threats that can help them breach the security barrier around any application environment. Luckily, there are ways in which we can keep these cyber threats at bay.

Application security risks can be managed in a streamlined manner, just like other information security threats. Through this book, we hope to have made you aware of the different kinds of potent application security risks and how they can be managed through a consistent and thorough pipeline of application security risk assessment, container security risk assessment, and remediation of the risks detected through these assessments. In the end, we also discussed how BizzSecure's EAID solution can help you manage application security risks in an automated and easy-to-use manner.

Overall, given the importance of applications in aiding the business operations of all organizations, their security should not be overlooked. Follow the steps that we have detailed in the various sections of this book to manage the application security risks in your organization. Subscribe to BizzSecure's EAID solution to integrate your entire application security management workflow onto a single automated platform.

Contact Us:

info@bizzsecure.com

1(833) 249-9732

www.bizzsecure.com