Vonage Business

Principles for Security in Customer Data

By ALYSSA MAZZINA

Oil spills cause outrage. It's easy to see their impact: sea birds covered in thick brown sludge put the environmental damage into a relatable context.

So, if data is the new oil, isn't it about time that we took data breaches as seriously?

In 2017, 2.3 billion credentials were leaked. And, while the EU's GDPR now makes data security nonchalance more risky, it took an average of 15 months between breaches happening and the responsible company owning up.

Whether you have hundreds or millions of customers, there are five security principles that you should follow to help ensure your organization is taking customer data security seriously.

Store Only What You Need

You can't leak data that you don't have. One of the first steps in ensuring the security of your customer's data is to store only what you need in order to serve them.

It can be tempting, though, to capture and store data that might be useful in future but for which you have no current need.

Imagine, for example, that you run an online store that sells fitness gear. Perhaps your ambition is to sell health supplements that you hope will appeal to the same people. So, you offer discounts to customers who share their average weekly menu with you. Then you analyze the data and identify potential dietary deficiencies. You don't need that data yet but it might be useful in targeting people when you launch your supplements business.

The next month, your website suffers a data breach. The criminals now have detailed information not only on what you need to run your fitness gear business but also on what your customers eat and your suppositions about whether they have a poor diet.

This seems like a trivial matter, but the same principle applies to businesses of all types. If you don't need it, don't collect it.

If you have customers in the European Union, you should have been thinking about data minimization since the GDPR came into force as it's a key principle of the regulation.

Default to Minimal Access

You can have the strongest possible hardware and software security but your customer's data is only as secure as your staff. MWR InfoSecurity conducts phishing tests for clients in a variety of industries.

On aggregate, 24% of staff clicked a fake social media connection request link. Of those, 54% then entered security credentials into the fake social media site. You might think that social media credentials couldn't cause too much harm but Panda Security reports that 52% of people reuse passwords across different services.

More worryingly, 18% clicked the link when presented with what appeared to be an email from their HR department inviting them to take an appraisal; 74% of those people entered their credentials in the fake appraisal system. If those had been genuine phishing attempts and the HR system and customer data of the affected companies sat behind the same single sign-on, then the phishers would have gained access to whatever data that employee had.

Giving people access only to what they need in order to do their job is a key principle in minimizing your data security risk. Think of it as operating on a need to know basis.

Train and Test for Security

You can reduce your risk by restricting data access only to those who need it. But what can you do when those people happily click on phishing links?

First up, security must become an integral part of your staff training. Instill the idea that customer data is like an unexploded bomb. It's safe enough if it is handled in the right way but if it isn't treated with the right respect then it has the potential to do enormous and irreparable damage. Train not only against phishing, and other social engineering, attacks but also to understand that working with customer data is a privilege.

Next, test that your defenses are working. Third-party companies can test system security through penetration testing: they'll mount an offense against your systems and then report back on the weak spots they found. And, as we saw above, similar testing is available to check if your staff are vulnerable.

Employ Multiple Layers of Security

It's not enough to have just one layer of security. The phishing examples above show that usernames and passwords can fall into the wrong hands.

A relatively simple way to mitigate such attacks is through two-factor authentication (2FA). Then, even if a staff member's credentials fall into the wrong hands they're only useful if the criminals also have access to the device used for 2FA.

For especially sensitive data, you should limit network access to that data only to the devices of staff who have permission to see it. By limiting access to certain IP addresses on your network, for example, you'll further reduce the potential for staff-driven attacks.

And, of course, you encrypt your customer data, right?

Plan for Failure

No matter how good your security, you should behave as though a breach is inevitable. By building your systems defensively, you'll minimize the fallout should a leak occur.

Planning for failure starts with having a clear procedure for what happens when a breach occurs. Your process should cover:

- **Lock-down:** restrict access as much as possible, and maybe entirely take systems offline, until you're certain that you understand what has happened and that the attack vector has been neutralized.
- **Reset:** change all system passwords and, if appropriate, affected customer passwords.
- **Determining and prioritizing what data was affected:** you must be aware of the scope of the breach as early as possible.
- **Tell the people who need to know:** inform your local data protection authority, tell banks if card numbers were stolen, be prepared to speak to the press if they contact you and, most importantly, be completely transparent with customers.
- **Clear roles and responsibilities:** executing your plan is a matter of everyone knowing where they fit in and, just like any other emergency situation, you need to rehearse frequently in order to minimize delay when it happens for real.

The internet can be a hostile place and it's no wonder when data is so valuable. Precisely how you protect from attack will be different for every organization. However, by starting with these principles you'll give your company the right basis from which to look after your customers' data.

Please fill out the form and we will be in touch with you shortly.

1.844.324.0340

First Name

Last Name

Email Address

Phone Number

Are you a Developer?

Company Name

Select Country

Product of Interest

Existing traffic to switch?

Traffic Volume Monthly (Optional)

Message (optional)