RANSOMWARE

Kronos Ransomware Attack Reveals How Your Customers Will React

By Bruce Sussman

Read more about the author

TUE | DEC 14, 2021 | 10:46 AM PST

Here is some vital information for your next incident response tabletop exercise.

This information *is not hypothetical*, instead, *it is unfolding* in real-time as a major player in the human resources industry responds to a ransomware attack.

Fallout from the attack is revealing the types of questions your customers and clients will ask you. And also what they will post about you as they critique your incident response.

One thing is becoming clear in this case: a successful cyberattack can instantly drag your reputation down.

Most Recent

IR lessons from the Kronos ransomware attack

HR timekeeping and payroll service Kronos was on a roll.

It successfully merged with another company to become Ultimate Kronos Group, it recently hired more than 1,200 new employees, and it sped up its innovation pipeline for its services.

But this week, the company announced a ransomware attack against its cloud-based services. And the announcement detailed stunning news. *It could be weeks* before services are restored.

> "While we are working diligently, our Kronos Private Cloud solutions are currently unavailable. Given that it may take up to several weeks to restore system availability, we strongly recommend that you evaluate and implement alternative business continuity protocols related to the affected UKG solutions."

This left HR, IT, and cybersecurity teams with a lot of unanswered questions. And they are posting about it on the Kronos user group page.

As our SecureWorld News team reviewed these, it became clear: these are the types of questions your customers will pose, post, and share if your organization gets hit with a cyberattack.

Kronos ransomware attack: what about business continuity?

Your customers may publicly post about your business continuity plan (BCP) or speculate about whether you have one.

In the case of the Kronos ransomware breach, this started with a key question: will the Kronos cloud really be down for weeks and if so, how is that possible?

Curtis wrote:

> "I understand that an accurate ETA may not be

CYBERSECURITY

They Made $30 Million Because Hackers Showed Them the Future

Most Popular

CYBER LAW

Suing the CISO: SolarWinds Fires Back

More Like This

RANSOMWARE

Putin Advisor: 'Military Activities in Cyberspace Are in Full Swing'

> available but I am really looking to find out if it will be several WEEKS? That may be worst case scenario OR is it a real possibility that it will be down for weeks? If so, that is very concerning!"

Tacomageorge wondered out loud: don't you have a business continuity plan?

> "It is extremely disappointing how this has been handled. The fact that Kronos response to all of us is to implement our organization's current Business Continuity plan, yet they don't have one. Additionally, they are not providing us w/ any type of solution to install locally so that we can gather our data. I know that we will be unable to wait "several weeks" for a solution for our timekeeping. Why did I renew my support when I am not receiving any?"

efujioka2 posted:

> "I am disappointed that UKG being the size they are and all they promote there was no Plan b, c, d etc. for such a situation."

Traci responded to that comment:

> "Yes! I'm kicking myself for not doing my own daily data backups. To lose access to all of our prior pay period data (bank file due this Wed), and all access to future pay periods, without notice, at year end, is an epic disaster, apparently without a business continuity plan!"

Kronos ransomware attack: customers ask about cyberscurity

Beyond wondering about your continuity planning and possible downtime, customers are likely to ask for information you may not even have for some time. On the Kronos chat board, some asked about the cybersecurity of their data.

Barani wrote:

> "Knowing this is a ransomware attack, do we have a word on data security? Any idea if our data is compromised or lost? This information will help initiate risk & communications at our side. Please shed more light on our data."

And you can certainly expect questions about your backups. See what *chsalcedo* wrote to the Kronos user group:

> "Where are the backups, can't the backups be restored? Are the backups stored in the same "cloud/space" as production, that doesn't make sense? A few weeks to be back up and running is unacceptable!"

Others will share what they are doing to mitigate the cyberrisk from your compromised network or service. *Ron* posted this:

> "One thing we are doing is reapplying firewall rules to disallow traffic to/from the devices within our own network. Can any of you tell me what other precautionary measures you are taking at your company?"

And Gene chimed in as well:

> "We are blocking/disabling all ADFS and LDAP connections to UKG/Kronos Cloud until they have a better handle on what they have. At this point they are an untrusted entity and will be treated as such. There is no good they can do us at this time."

Kronos ransomware attack: posts about pain this will cause

You will also want to plan for questions relating to how you serve your customers, and how that trickles down to real-world impacts. In other words, *your* data breach…*their* pain.

A Kronos customer posted this this:

> "This is going to be a huge hardship for our employees that depend on the premium pay such as night diff, meals, overtime, Our timekeepers have no way to track the hours from 12/1/21 to today. Some employees work the extra OT to pay loans, cars loans, credit cards and home loans, insurance etc. Missing payments will effect their credit ratings for years."

This is another example of how ransomware attacks impact real life. And Kronos and its brand reputation are caught in the middle of it all.

Here is where you can read the Kronos announcement and the customer posts.

Are you ready for these types of questions? Have you looped in your communications folks as part of incident response planning? Any suggestions on how to do this successfully?

If so, please post in the gated comments, below.

Ransomware Lifecycle Podcast

The Kronos ransomware attack brings to mind a powerful keynote at a SecureWorld conference.

Cybersecurity attorney Shawn Tuma of Spencer Fane, took us step by step through the ransomware lifecycle. He explains how your organization can go from 'on-top of the world' one moment to the 'sky-is-falling' the next. And how to recover from that point. Give it a listen, here:

Tags: Ransomware, Business Continuity Plan

Comments

First Name*

Last Name

Email*

Comment*

protected by reCAPTCHA
Privacy - Terms

Submit Comment

See what SecureWorld can do for you. Contact us today! CONTACT US

First name*

Email address*

SUBSCRIBE