endsight

CrowdStrike Executive De-Brief

Presented by Endsight

1144 Jordan Lane Napa, CA 94559
(510)280-2000
info@endsight.net
www.endsight.net

endsight

Stephen Hicks

CISSP, CCSP, CISM

shicks@endsight.net

Security Practice Manager @ Endsight

About Endsight

- Founded in 2004
- IT, Cybersecurity, Cloud, and Microsoft 365 consulting
- Based in Napa with an office in San Diego
- We provide these briefings and free trainings to the community at large without sales intent. A rising tide lifts all ships.

endsight

Up to date Crowdstrike notes

- Not an attack - a misconfiguration and a bad patch.
  - No inherent risk to data, systems, identities.
- Two issues – one at Microsoft and one at CrowdStrike.
- Microsoft had a configuration issue late Thursday night.
- Crowdstrike sent a bad update to their customers.
  - This update is crashing computers worldwide.
  - The fix for these crashes is particularly challenging.
    - A catch-22 for systems with certain configurations.
- Remote fixes are in early stages of testing and are not certain yet.
  - This is a major challenge for IT firms and Fortune 500 organizations.

endsight

Who is Crowdstrike?

- Crowdstrike is a leading security software vendor
- Falcon is their endpoint protection platform
  - Falcon is one of the major leaders in the endpoint protection space
  - Combination of EDR/Monitoring/Other security tooling
- What is an EDR?
  - Modern antivirus with Artificial Intelligence.
  - Required by most insurance and all regulatory organizations.
  - Extremely important component in technological protection.

endsight

Impact

- This situation may take weeks to correct if it’s necessary to physically access computers.
- Several Fortune 500 companies are still reporting >20k computers down.
- There is no risk to client data/systems/identities inherent to this situation. The major risk is downtime and opportunity cost.

endsight

Endsight's Stance

- Endpoint protection agents have more power (and thus more risk) on Windows and Linux systems
  - This comes with performance benefits (protection is faster on these systems) as well as protection benefits (there's no way for an attacker to have 'deeper' access than a defender).
  - This also comes with risks – drivers and configuration files with very deep access to computers can cause these crashes.
  - Microsoft has an agreement with the EU that requires this setup.
- EDR and other endpoint protection is *critical* in a production environment for *all* organizations.
- This situation will occur again – hopefully not at the same scale.

endsight

Endsight's Stance Continued

- Endsight vets all software vendors with which we have agreements.
  - This helps to minimize these incidents but can never eliminate them.
- Incidents like this one (a bad update or similar) are not exclusive to Crowdstrike or any other software vendor
- BC/DR plans are very important. This is as much a 'disaster' as any natural or other man-made situation.
- For MSPs that support hundreds (or thousands) of clients, supportability, accountability, and Service Level Agreements are more important than the newest technology.
  - Crowdstrike is not a startup.
- Cloud migrations and less reliance on onsite systems are strategically important for resilience.

FREE 60 minute
Cybersecurity Fundamentals Training
by endsight

TO SIGN UP

scan the QR Code with your camera phone

-or-

go to https://get.endsight.net/monthly-cybersecurity-fundamentals-training

2nd Tuesday of each month
1 PM PST

***Endsight does this LIVE webinar training monthly. Occasionally, we need to move the training to another day.**

You will learn

- How to work securely anywhere
- How to better spot phishing attacks
- The best cyber safety practices

Upcoming Sessions: Office Hours

- **August 22nd!**
- **Topic: Recent events this quarter**

- Great for business leaders and tech professionals, also for anyone looking to stay up to date on recent cybersecurity trends.
- Extensive Q&A - if you have a question, we'll get it answered! We can also take sensitive questions offline.
- This will be recorded, so if you can’t make it, you'll receive a recording!
- Registration link is in the comments.
- Reply to our follow up email or email akreps@endsight.net to register.

endsight

Thank you!

1144 Jordan Lane Napa, CA 94559
(510)280-2000
info@endsight.net
www.endsight.net