Current State of Cybersecurity: The August Schell Perspective

The cybersecurity experts at August Schell have responded to the onslaught of ransomware attacks, witnessed the increasing risks pervading the industry, assisted customers with internal barriers to better security, and recommended technologies that make businesses safer.

In working closely with the top experts in cybersecurity, as well as our customers, we've put together a list of the top fears, trends, and risks we've observed this year.

PRIMARY RISKS

Your Employees
Data Loss
Ransomware

ORGANIZATIONAL ROADBLOCKS TO ENHANCING SECURITY POSTURE

Lack of Internal Resources and Siloed Organization Structures

Demand for cybersecurity expertise has skyrocketed, and the need will continue to grow.

Meanwhile, IT, security, and compliance often don't operate as a team, which prevents people from working together effectively to solve problems.

Moving Too Slowly

It's common for vulnerabilities to exist on a system unchecked for months (and in some cases years). Even in the case of attacks that happen fast, such as ransomware, security teams often lack an equally fast response.

Adhering to Old Processes

28% of businesses report that compatibility problems with legacy systems are the biggest barrier to adopting advanced security technology and processes.[1]

WHAT YOUR PEERS ARE WORRIED ABOUT

Lack of Security Preparedness or Awareness

Federal agencies and enterprises are fighting on a complex cyber battlefield, and many worry they lack the preparedness to combat threats—research confirms the validity of this fear.

The Internet of Things (IoT)

Internet of Things (IoT) is replacing mobile as the emerging area of concern, and fears are increasing significantly, ISACA noted.[2] Most businesses who work with the IoT have major worries about the vulnerabilities of connected devices, as well as a lack of security by design.

Responding to New Threats, Where Current Tools Are Ineffective

Organizations know new threats are ample, but responding requires new tools and methods. Signs of a weakening focus on operationalization shows that organizations aren't ready to defend a growing attack landscape.[1]

TOP CYBERSECURITY MISCONCEPTIONS

- "The Silver Bullet"
- We're Safer Than We Really Are
- Software Alone Can Solve Every Cybersecurity Problem

LOOKING TO THE FUTURE: WHAT YOU SHOULD KNOW

"We are always trying to invent better ways of protecting against cyber threats, and there are many facets to cybersecurity: protecting people's identity, their data, the businesses data, and more. There are also multiple ways for the bad guys to try to subvert this information, from insider threats to elaborate phishing schemes. "

-Ron Flax, CTO at August Schell

The Cybersecurity Problem Isn't Going Away Anytime Soon

Businesses must stay aware of current threats and the best practices that can be employed to defeat them, for today and tomorrow.

Most Cybersecurity Software Solutions Are Designed to Solve Specific Problems

Micro-segmentation implements firewalls between application components on the same network segment. Threat intelligence tries to evaluate log and machine data to detect anomalies and matches against signatures of known attacks. Don't forget "The Silver Bullet" fallacy, and use the appropriate tools and solutions to form a holistic strategy.

There Are Simple Security Measures Businesses Can and Should Take

- Consistent patching practices
- Stronger password practices
- Using 2FA
- Minding separation of concerns

TECHNOLOGY YOU SHOULD STRONGLY CONSIDER

Big Data/Machine Learning Tools

The power behind big data has been proven, as have machine learning capabilities.There are many excellent tools available; here are a few we work with frequently at August Schell:

- Splunk
- Zoomdata
- Recorded Future

Network Virtualization & Virtual Network Security

The legacy approach to networking is being replaced with an approach that enables agility and speed and empowers hybrid-forward, cloud-native focused organizations: network virtualization. Alongside the virtual network comes virtual network security capabilities. We recommend VMware NSX.

PKI/Identity Management

PKI is critical to the foundation of a strong security posture. It enables security teams to establish the identity of people, devices, data, and services. User IDs and passwords aren't enough.

August Schell Enterprises is committed to staying ahead of advanced threats and keeping pace with emerging technologies. If you have questions about what's coming up for your business on the security horizon, or would like to assess your security posture, reach out to an August Schell expert today, or call us at (301)-838-9470.

References

1. Cisco, "2017 Annual Cybersecurity Report," January 2017.
2. ISACA, "State of Cyber Security 2017: Part 2: Current Trends in the Threat Landscape," 2017.

augustschell