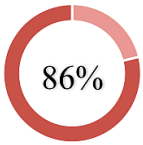
FACTS ABOUT DATA BREACHES AND RISKS TO YOUR BUSINESS

Bypass Firewalls and IDS/IPS Systems



Today's advanced threats bypass firewalls and use encryption to make IDS/IPS systems useless. A massive 86% of threats go right through these systems.

In other words, nearly 9 out of 10 of threats aren't stopped by the traditional systems you're probably relying on today. Fact is, if you are not continuously monitoring your network, servers, and data, you could be a victim of a data breach without even knowing until it's too late.

Cost of a Breach

$3.75M

The average cost of a data breach is now $3.75M. Imagine the impact to your business of a breach costing even half or a quarter of that amount.

And this number is an average for all types of data breaches. If your organization processes credit cards, or has other sensitive data such as health records and financial information on customers or employees, this cost would be *much* higher.

Days to Detect

205

On average, successful breaches go undetected for 205 days - that's over 7 months! This is what happened in high profile breaches like Sony, Target, and Anthem.

But the threat isn't limited to large organizations. It is now more valuable than ever to compromise small and medium size businesses, then quietly steal data and credentials over a long period of time. And these undetected breaches are the perfect way to steal the identities of your customers and employees.

HOLISTIC SECURITY MONITORING IS NO LONGER AN OPTION

By The Security Operations Center

Cybersecurity threats are on the rise and only getting more dangerous. It seems every day there's a new headline about another data breach. And it's no longer only large enterprises that must be concerned. Recent breaches have shown that small and medium size businesses are also highly vulnerable to today's threats, and the impact can be enormous. This is even more true if you fall under PCI, HIPPA, SOX, or FFIEC regulations where compliance is absolutely critical to avoid fines or worse.

Today's threats and compliance guidelines require organizations of all sizes to collect, correlate, and analyze security information from all IT systems to enable rapid detection and remediation. Without this continuous, holistic monitoring, critical security events from your servers, routers, and other network devices go unnoticed. A proper security monitoring solution can help answer critical questions that are vital to your cybersecurity protection – questions such as:

- A user login has failed multiple times; **did the employee forget their password or is this a brute force attack?**
- Sensitive files on a server were accessed last night; **is this normal business use or did we just get breached?**
- A typical firewall can send out 864,000 events per day; **how do I know which of these (if any) are important?**
- New wireless access points have been added to the network; **where are they and was this intentional?**
- Regulatory compliance requirements are changing constantly; **do we have the data needed to properly comply?**

MEDICUS IT

We do 'IT' Right!

Contact us today:

678.495.5901

www.medicusit.com