Your next breach:

3 cyber threats that are hitting businesses like yours

vodacom business

Introduction

What's the one thing more dangerous than a cyberattack? **Not knowing it's already happening.**

Right now, your business is a target—not because of what you've done, but because of what you haven't seen. Cybercriminals don't storm in with sirens blaring. They sneak through the cracks—your inbox, your cloud, your team's everyday habits—exploiting trust and routine until it's too late to stop them.

A phishing email disguised as a vendor request. A **malware-laced attachment** in an employee's inbox. A **cloud misconfiguration** leaving **confidential data exposed.** These aren't hypothetical risks—they're some of the **most common ways businesses get breached.**

And your challenge isn't just stopping known threats. It's protecting against the ones you haven't even considered yet.

In this guide, we'll break down the **three biggest security gaps** most businesses overlook, and how you can **protect your business** against them.

vodacom business

Threat #1: Phishing and email attacks

Cybercriminals don't need to hack their way into your business. They just need one employee to click.

Phishing attacks have evolved far beyond the obvious scams of the past. Today, cybercriminals use highly targeted, sophisticated emails that look like legitimate business communications. That's why they're the number one cause of data breaches worldwide.

It could be:

An invoice from a supplier
except the bank details have been swapped.

A security update from Microsoft
except it leads to a fake login page.

An internal request from your CEO
except the email has been spoofed.

Phishing attacks work because **they don't look like attacks at all.** They exploit **trust, routine, and human error.**

The impact on your business

A single phishing email can:

Steal login credentials,
giving attackers direct access to critical business systems.

Inject malware,
leading to ransomware injections or data theft.

Trigger financial fraud,
with fraudulent payments sent before anyone realises what happened.

By the time you realise what's happened, **the damage is already done.**

vodacom business

Threat #2: Ransomware

A ransomware attack doesn't just steal your data—it takes it hostage.

It only takes one infected file, one outdated system, or one unprotected device for ransomware to spread through your entire network. Once it's inside, it encrypts everything—locking you out of your own business unless you pay.

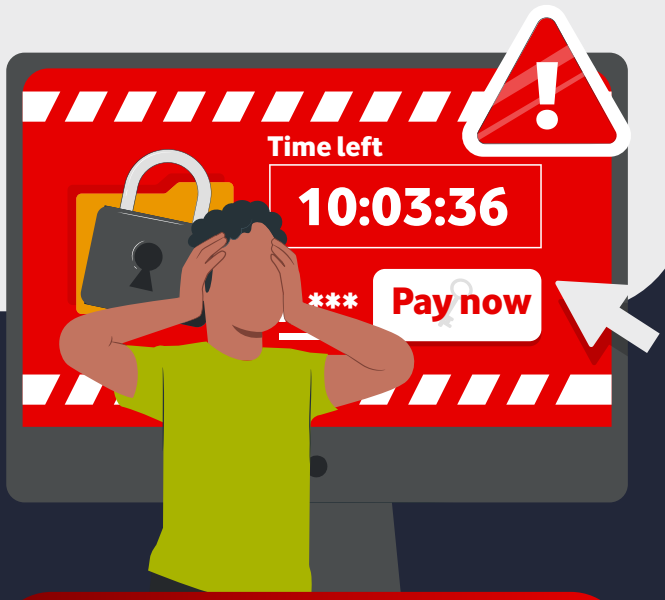
How does it get in?

A simple email attachment
a fake invoice or contract loaded with ransomware.

An outdated system vulnerability
a gap in security that hackers exploit to break in.

Weak remote access credentials
attackers using stolen or brute-forced passwords to gain

Ransomware doesn't just infect a single machine. It spreads. It moves across networks, locking files, disrupting operations, and forcing businesses to either pay up or start over.



And even if you do, there's **no guarantee** you'll get your data back.

The impact on your business

A single ransomware attack can:

Shut down critical operations,
making files and systems completely inaccessible.

Cost thousands
or millions – in ransom payments, downtime, and recovery costs.

Permanently destroy data
if backups are also compromised.

And the worst part? **Ransomware attacks** aren't just targeting **large corporations** anymore. **Small to medium businesses** are now **prime targets** because hackers know they're often **unprepared.**

vodacom business

Threat #3: Cloud misconfigurations

Not all cyber threats are the result of an attack. Sometimes, businesses leave the door open themselves.

Cloud services have made operations faster, more flexible, and more scalable. But with that convenience comes a major security risk—misconfigurations, weak access controls, and overlooked vulnerabilities that expose sensitive business data.

And attackers don't even have to break in—**they just find what's already exposed.**

Where do cloud security gaps happen?

Misconfigured storage settings

A cloud database accidentally left public instead of private. except the bank details have been swapped.

Weak or stolen credentials

Attackers gain access through leaked passwords or unsecured login portals.

Excessive user permissions

Employees or third-party vendors have more access than they should, increasing the risk of insider threats or accidental exposure.

A single **misconfiguration** can mean customer data, financial records, or proprietary business information is sitting in the open—**available to anyone who knows where to look.**

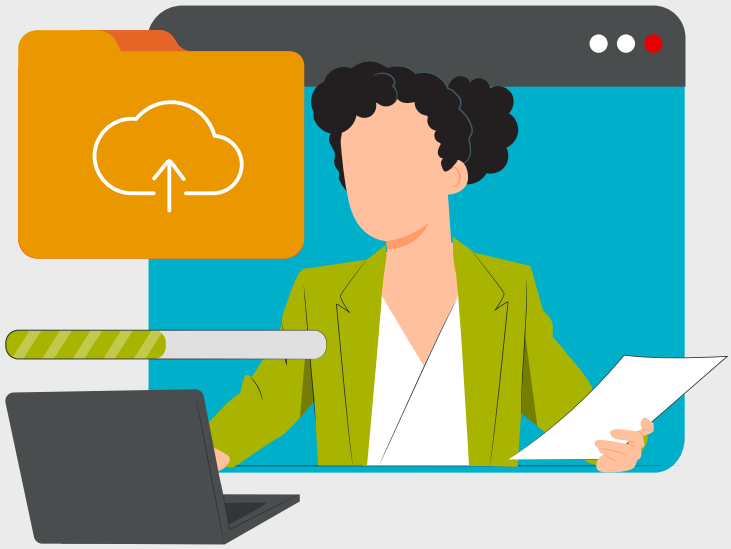
The impact on your business

A single phishing email can:

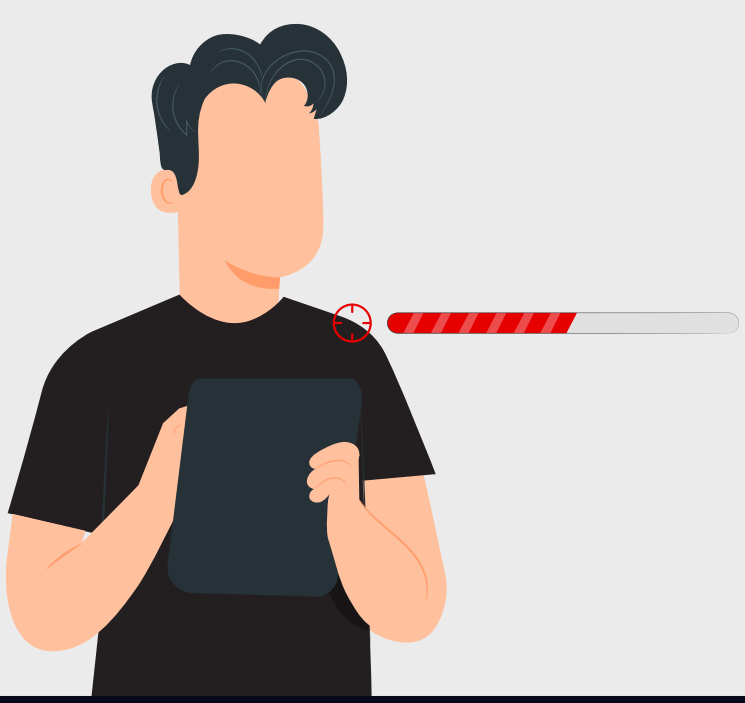
Expose confidential business data,
leading to regulatory fines and reputational damage.

Give attackers full access to your systems,
enabling further breaches and insider threats.

Cause financial loss,
either from direct data theft or legal consequences.



vodacom business



Most businesses don't realise their **data is exposed** until **someone else finds it first.**

How Vodacom Business can help

New threats emerge daily. And while you can't predict what cybercriminals will come up with next - you can be ready for it.

Trend Micro protects against the **most** common **cyber threats**—phishing, ransomware, cloud vulnerabilities—**all in one affordable, enterprise-grade solution.**

It gives you:

AI-powered threat intelligence

continuously adapts to new attack patterns, detecting phishing scams and zero-day threats in real time.

Behaviour-based ransomware protection

that not only blocks known malware—it stops suspicious encryption processes before damage is done.

Automated cloud security

detects misconfigurations, enforces access controls, and scans for anomalous activity before it leads to a breach.

It's a **cost-effective way** to secure your business from **all three major cyber risks—without complexity or high costs.**

vodacom business


vodacom
business