

Analisis Perbandingan Harga Saham Dan Volume Transaksi BRIS Pada Masa Sebelum Dan Sesudah Serangan *Ransomware* (Studi Kasus Pada PT Bank Syariah Indonesia, Tbk. Pada Tahun 2023)

DESKRIPSI

Bank Syariah Indonesia (BSI), kini menjadi bank syariah terbesar di Indonesia. Namun beberapa waktu lalu BSI mengalami terhentinya beberapa layanan, salah satunya yaitu mobile banking. Hal ini disebabkan oleh serangan ransomware, yang pada dasarnya serangan ini bekerja dengan cara mengunci akses data, sehingga jalannya operasi suatu bisnis dapat terganggu. Selain itu, fenomena ini berdampak juga pada penurunan saham BSI dengan kode BRIS. Tujuan pada penelitian ini untuk mengetahui perbedaan harga saham dan volume transaksi saham BRIS pada masa sebelum dan sesudah serangan terjadi.

RUMUSAN MASALAH

- Apakah terdapat perbedaan yang signifikan dari harga saham BRIS pada masa sebelum dan sesudah serangan ransomware yang terjadi pada tahun 2023?
- Apakah terdapat perbedaan yang signifikan dari volume transaksi saham BRIS pada masa sebelum dan sesudah serangan ransomware yang terjadi pada tahun 2023?



METODE PENELITIAN



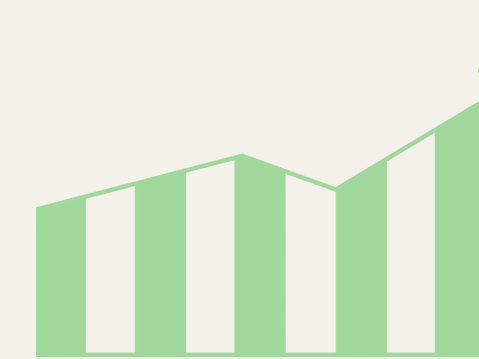
JENIS PENELITIAN

Menggunakan metode kuantitatif dengan pendekatan komparatif



SUMBER DATA

Sumber data menggunakan data sekunder yang didapat dari website www.finance.yahoo.com dan www.idx.co.id



POPULASI DAN SAMPEL

Populasi : PT. Bank Syariah Indonesia, Tbk
Sampel : Harga Saham dan Volume Transaksi BRIS



TEKNIK PENGUMPULAN DATA

Data 50 hari sebelum dan sesudah serangan ransomware dengan sampel data harga saham dan volume transaksi saham BRIS



TEKNIK ANALISIS DATA

Menggunakan Analisis Deskriptif, Uji Hipotesis dan Uji Normalitas

Analisa dan Hasil

“Harga Saham BRIS”

| | | Paired Samples Test | | | | | | | |
|--------|---|---------------------|----------------|-----------------|---|---------|--------|----|-----------------|
| | | Paired Differences | | | | | | | |
| | | Mean | Std. Deviation | Std. Error Mean | 95% Confidence Interval of the Difference | | t | df | Sig. (2-tailed) |
| | | | | | Lower | Upper | | | |
| Pair 1 | Harga Saham Sebelum Serangan Ransomware - Harga Saham Sesudah Serangan Ransomware | -45,600 | 104,733 | 14,811 | -75,365 | -15,835 | -3,079 | 49 | ,003 |

“Volume Transaksi Saham BRIS”

| | | Ranks | | |
|---|----------------|-----------------|-----------|--------------|
| | | N | Mean Rank | Sum of Ranks |
| Volume Transaksi Saham Sebelum Serangan Ransomware - Volume Transaksi Saham Sesudah Serangan Ransomware | Negative Ranks | 7 ^a | 20,93 | 146,50 |
| | Positive Ranks | 41 ^b | 25,11 | 1029,50 |
| | Ties | 2 ^c | | |
| | Total | 50 | | |

Test Statistics^a

| | | |
|---|------------------------|---------------------|
| Volume Transaksi Saham Sebelum Serangan Ransomware - Volume Transaksi Saham Sesudah Serangan Ransomware | Z | -4,529 ^b |
| | Asymp. Sig. (2-tailed) | ,000 |

Kesimpulan

- Serangan ransomware yang terjadi pada BRIS pada tahun 2023 memiliki implikasi, yang mana ransomware ini merupakan perangkat lunak berbahaya yang mengenkripsi data dan meminta tebusan untuk memulihkannya. Dalam pandangan Islam serangan ransomware dianggap sebagai pencurian dan melanggar prinsip hak milik.
- Dampak serangan ransomware yang terjadi pada BSI ini, selain mengakibatkan gangguan layanan, harga saham dan volume transaksi juga mengalami penurunan.
- Berdasarkan hasil uji harga saham BRIS menggunakan *Paired Sample T – Test* membuktikan ada perbedaan yang signifikan antara harga saham BRIS pada masa sebelum dan sesudah serangan ransomware.
- Sedangkan volume transaksi BRIS, dari hasil uji *Wilcoxon Signed Ranks Test* membuktikan ada perbedaan yang signifikan antara volume transaksi saham BRIS pada masa sebelum dan sesudah serangan ransomware.
- Perbedaan yang signifikan terhadap harga saham dan volume transaksi saham dapat disebabkan oleh beberapa faktor, seperti kekhawatiran investor terhadap dampak serangan ransomware terhadap kinerja keuangan BRIS, penurunan kepercayaan investor terhadap keamanan sistem informasi BRIS, serta peningkatan risiko investasi BRIS
- Untuk mengatasi dampak serangan ransomware, perusahaan harus memulihkan kepercayaan publik dengan memperkuat data dan sistem, serta perlu adanya antisipasi keamanan untuk mempersiapkan diri, sehingga dapat mengurangi dampak buruk dari serangan ransomware.